International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 1, February 2024, pp. 1135~1146
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i1.pp1135-1146

Enhancing healthcare services through cloud service: a systematic review

Bo Guo[1,2], Nur Syufiza Ahmad Shukor[1], Irny Suzila Ishak[1]
[1]Department of Computing, Faculty of Communication, Visual Art and Computing, Universiti Selangor, Selangor, Malaysia
[2]Department of Computer Science, Faculty of Computer and Information Engineering, Fuyang Normal University, Fuyang, China

Article Info

Article history:

Received Jun 29, 2023
Revised Sep 26, 2023
Accepted Oct 9, 2023

Keywords:

Cloud computing
Cloud services
Clustering analysis
Healthcare services
Systematic literature review

ABSTRACT

Although cloud-based healthcare services are booming, in-depth research has not yet been conducted in this field. This study aims to address the shortcomings of previous research by analyzing all journal articles from the last five years using the preferred reporting items for systematic reviews and meta-analyses (PRISMA) systematic literature review methodology. The findings of this study highlight the benefits of cloud-based healthcare services for healthcare providers and patients, including enhanced healthcare services, data security, privacy issues, and innovative information technology (IT) service delivery models. However, this study also identifies challenges associated with using cloud services in healthcare, such as security and privacy concerns, and proposes solutions to address these issues. This study concludes by discussing future research directions and the need for a complete solution that addresses the conflicting requirements of the security, privacy, efficiency, and scalability of cloud technologies in healthcare.

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

Corresponding Author:

Nur Syufiza Ahmad Shukor
Department of Computing, Faculty of Communication, Visual Art and Computing, Universiti Selangor
Bestari Jaya Campus, Street Timur Tambahan, Bestari Jaya, Selangor, Malaysia
Email: nur_syufiza@unisel.edu.my

1. INTRODUCTION

Cloud computing [1], [2] has recently attracted a lot of interest from the community and many scholars, owing to it is unique characteristics. Based on cloud computing technology, cloud services centralize and virtualize computing resources, enabling users to access and use these resources over a network without having to own or maintain computing equipment and infrastructure [3]. Cloud services can also allow for flexible provisioning of computing resources and services based on user needs and usage, and a pay-as-you-go model that allows users to only pay for actual usage, reducing user costs and risks [4], [5]. Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) are common service models in cloud services that can meet the needs of different users and application scenarios [6], [7].

In recent years, the ease of using cloud services in healthcare has attracted significant interest from governments, research communities, and numerous sectors. Cloud-based healthcare services allow healthcare providers and doctors to provide online consultations, remote diagnoses, and medical advice to patients via the internet [8]. Simultaneously, patient medical and health data can be uploaded to cloud platforms for centralized management and analysis, providing providers and doctors with more comprehensive and accurate healthcare services [9]. Healthcare services in the cloud can also facilitate the sharing and collaboration of healthcare resources, improve the efficiency and quality of healthcare services, reduce medical costs, and improve people's health and healthcare experience [10]. Thus, cloud services offer great value to healthcare organizations and play an important role in achieving operational efficiency, patient safety, and staff content in the healthcare industry [11]. In addition, cloud computing organizes patient healthcare histories and medication biographies to provide an effective framework for the rapid use of patient healthcare records [12]. Currently, cloud healthcare services are widely used and promoted as an important trend in future healthcare services [13].

A systematic literature review (SLR) is a method used to answer a specific research question by systematically searching, screening, evaluating, and integrating existing research literature to identify, analyze, and synthesize all research pertinent to a certain research topic or noteworthy trend [14]–[16]. SLR can provide an in-depth understanding of a nature of the research question, identify the strengths and flaws of previous research, and provide directions and recommendations for future research by screening and integrating a vast body of relevant literature [17]. SLR has a clear research question, transparent search strategy, and rigorous approach to literature screening, evaluation, and integration, which can reduce subjectivity and bias and increase the credibility and persuasiveness of research [18]. By systematically integrating and analyzing existing research results, SLR can avoid replication of research, waste of resources, and increase the effectiveness and efficiency of research [19]. Despite the widespread use of cloud-based healthcare services, no comprehensive research has been conducted in this field. Therefore, the objective of this study is to systematically investigate and evaluate the most recent methods in the area of healthcare services in the cloud.

The goal of this study is to review the impact of cloud services on healthcare. Although healthcare is an important application scenario for cloud services with a promising future, a survey of the existing research in this area reveals that there is no comprehensive or in-depth review. We were inspired to write this paper based on this gap. In summary, this study explored the current status and trends of healthcare services in cloud services and provided a thorough analysis of these services. Additionally, current research points to several future directions for this field of study.

The significant contributions of this study are as follows: i) Review of issues in health services in the cloud; ii) Prepare a thorough analysis of existing approaches to healthcare services in a cloud environment; iii) Examine use cases for cloud-based healthcare services currently available; and iv) Brief description of key application scenarios for cloud-based healthcare services in future research.

The rest of this paper is structured as follows: The existing literature on this study is introduced in section 2, and section 3 discusses the research methodology used. Section 4 provides an overview of this study's findings. Section 5 discusses the important issues. Finally, section 6 presents the conclusions of the study and discusses future research directions.

2. RELATED WORKS

Ali *et al.* [20] conducted a systematic review of academic literature on cloud computing in healthcare, and proposed a framework for classifying opportunities, issues, and applications. The implications for future research and practice include enhanced healthcare services, data security, privacy issues, and innovative information technology (IT) service delivery models. Al-Issa *et al*. [21] explored cloud computing's application in healthcare and the difficulties with security and privacy that come with it. The study concludes that there is a pressing need for a complete solution that addresses the conflicting requirements of the security, privacy, efficiency, and scalability of cloud technologies in healthcare. Usak *et al.* [10] reviewed literature on internet of thing-based (IoT-based) healthcare services and highlighted the benefits, drawbacks, and challenges of these mechanisms. The authors discussed the need to further understand the opportunities and issues associated with IoT-based healthcare systems and to provide valuable insights for practitioners and researchers. Research has shown that the IoT can help governments improve healthcare services and business interactions in society. Rahimi *et al.* [16] conducted a systematic study on service selection methods for cloud services. The selected papers were classified into three main categories and studied based on the important qualitative parameters. It was found that decision-making, metaheuristic, and fuzzy-based methods have advantages and limitations in the service selection for cloud services. A high level of security and privacy is required for health records when cloud computing is used in eHealth [22]. However, this also raises severe issues regarding private health information. Practical and efficient security and privacy management techniques are crucial to address these concerns. This paper reviews the current topics of study on privacy and security in eHealth clouds, analyzes and summarizes cutting-edge technologies and methods from 132 studies, and offers researchers rich knowledge and data on current developments in security and privacy research.

Although the above studies provide a solid foundation for scholars to better understand the various areas involved in cloud-based healthcare services, they have some shortcomings. Some studies did not cover recent years, others did not categorize application scenarios, others did not provide a clear literature screening process, and others did not provide security algorithms. To address these shortcomings, this study focuses on all journal articles from the last five years using an explicit paper selection process and further classifies application scenarios using a comparative discussion method. Finally, important metrics for evaluating the methodology are highlighted.

3. RESEARCH METHOD

This section reviews existing literature on healthcare services in the cloud using the SLR method. To comprehensively explore the relevant research, the research methodology used in this study is illustrated in Figure 1. The results of the automated search of existing studies published between 2010 and 2023 are shown in Figure 2.

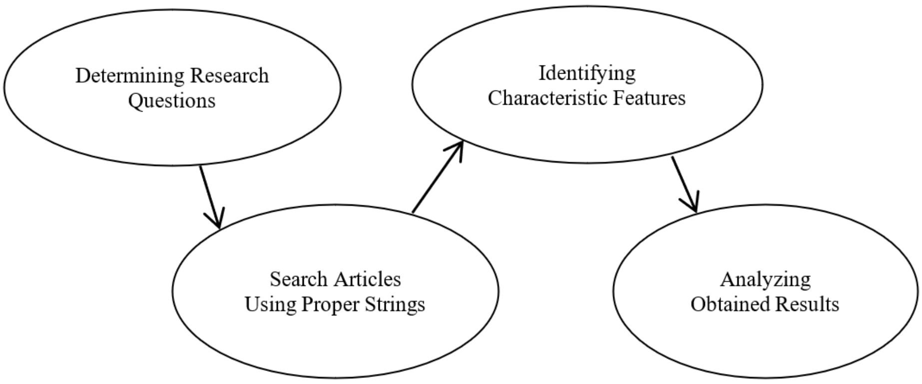

Figure 1. The selected research methodology

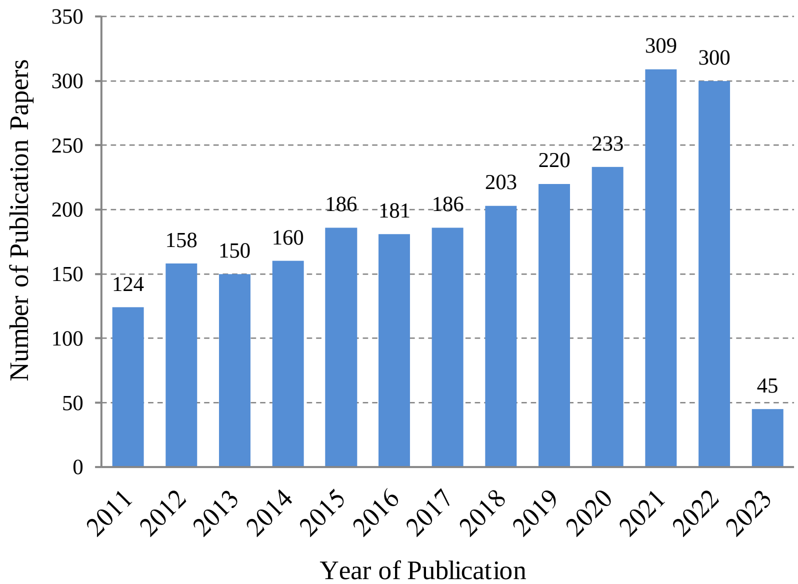

Figure 2. The number of published papers on healthcare services on the cloud

3.1. Question formalization

To further explore the topic, appropriate research questions are essential to answer the associated research objectives. The right research questions help guide the methodology, data collection methods, and interpretation of results. Therefore, a set of basic research questions was developed to guide research progress and better structure the SLR methodology. Three main research questions were identified for the research-related review articles and will be applied to the selected techniques in later chapters. These questions contribute to a better understanding of the topic covered. The questions are as follows:

Question 1: What are the key parameters for evaluating cloud-based healthcare services?
Question 2: What are the main uses of healthcare services in the cloud environment?
Question 3: What are the unresolved problems in the field?

3.2. Search strategy

A further search of the Web of Science database was conducted to select relevant, high-quality studies. Following preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines, an exhaustive literature search was conducted in the Web of Science database, using the search string ((“healthcare facilities” OR “healthcare institutions” OR “healthcare space” OR “healthcare setting” OR “health” OR “healthcare service”) AND “cloud”). Only English-language articles published in journals during the 2019-2023 publication periods (last five years) were considered with context (content related to healthcare services in a cloud environment) and availability of full text.

3.3. Criteria for inclusion and exclusion

To select high-quality studies for review, we selected only academic journal papers on cloud-based healthcare services and eliminated other sorts of studies, such as surveys, working reports, book chapters, notes, review papers, and Ph.D. and Master’s theses. We surveyed on March 23, 2023, and used a well-established report of PRISMA statement. In the following, we outline the main steps based on the PRISMA statement as shown in Figure 3.

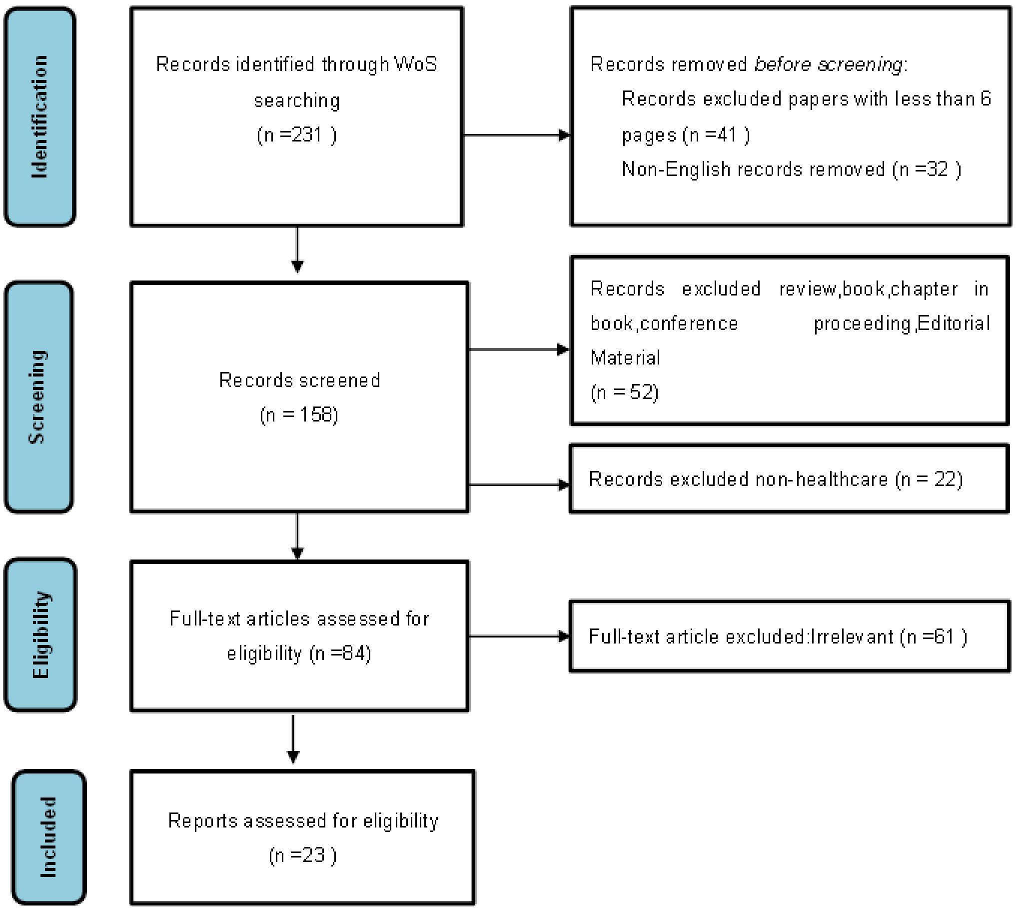

Figure 3. The flow diagram of PRISMA

To select papers that were appropriate for review and specifically addressed cloud-based healthcare services, a full-text review of all research papers was carefully completed. Table 1 summarizes the criteria for inclusion and exclusion used to add relevant articles and to remove irrelevant articles. Based on these characteristics, 23 papers were selected for further analysis.

Table 1. Inclusion and exclusion criteria of selected articles

Criteria	
Inclusion	Provide solutions for healthcare services in the cloud
	Discussing cloud-based healthcare services
	Explicitly specify research objectives
	Comparing the existing methods with the proposed method
Exclusion	Paper not written in English
	Work without technical content
	Review, working reports, notes, Survey, book chapter, Ph.D. and Master theses
	Extended abstracts (papers with less than 6 pages)
	Full text not available

4. REVIEW OF CHOSEN PAPERS

This section reviews the selected papers on the provision of healthcare services on cloud services and details their advantages and disadvantages. The selected studies were grouped into the following five categories: disease detection and treatment, electronic health record analysis, health management, and prediction, patient population analysis, and security and privacy protection. Figure 4 shows the classification of these studies and provides a brief description.

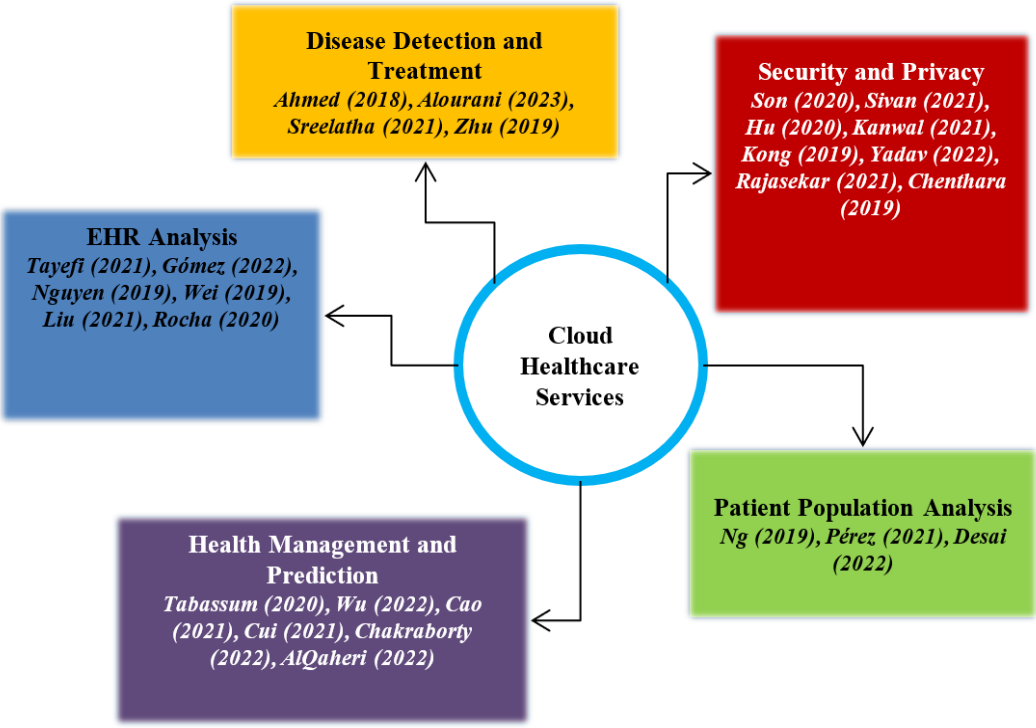

Figure 4. The classification of healthcare services on cloud services

4.1. Disease detection and treatment

Healthcare services on cloud services for disease detection and treatment refer to the applications of cloud computing technology in the healthcare industry to improve disease detection and treatment [23]. Cloud computing can manage, store, and process large amounts of medical data and allow healthcare practitioners to access these data anywhere. With the assistance of healthcare services in the cloud, doctors and researchers can collaborate more effectively, leading to a faster and more accurate diagnosis and treatment. Cloud-based healthcare services can also enable remote patient monitoring and telemedicine, making healthcare more accessible and convenient for patients.

Alourani *et al.* [24] presented findings and a comparison of mortality prediction using different machine learning algorithms that were utilized for particular features of the dataset. The criteria for the accuracy, recall, precision, and F1-score metrics were used to assess the models. According to the results, the deep neural network (DNN) performed better than the other models in the context of accuracy, recall, precision, and F1-score, achieving an accuracy of 80%, recall of 79%, precision of 86%, and F1-score of

80%. DNN performed better than the other models for all metrics evaluated. A machine learning model based on a DNN was proposed to predict patient mortality, and it showed better performance than other learning algorithms. However, the model has a long execution time, requires the consideration of additional measurement parameters and feature selection methods to obtain better results, and must be tested in an internet of thing-integrated (IoT-integrated) environment and integrated with other applications for validation.

Sreelatha and Reddy [25] suggested a new efficient integrity check scheme (EICS) method for the deduplication process and compared its performance with that of existing methods. The suggested method performs better than existing approaches in terms of storage-space utilization, processing time, and security level. The suggested method successfully implements a two-level encryption mechanism to improve security. The proposed method for keeping health records in the cloud includes generating an indexed table for each file, utilizing the support vector machine (SVM) algorithm to learn file characteristics and encrypting the indexing table through a two-stage encryption process before archiving it to the cloud server. This approach exceeds previous works with respect to execution time, storage space, and security level, and can be extended to other applications dealing with records in the cloud.

Zhu *et al.* [26] proposed a blockchain-based model for sharing cloud health services with consensus, resource sharing, international payments, and distributed ledgers. A simulation study on the detection of breast cancer was conducted and a recommendation system was created to locate the right provider for service inquiries. To counteract potentially biased ratings, a novel conciliation mechanism was created for the service assessment system. The proposed model has great potential, and future research is required to optimize it, address security issues, and explore new applications.

4.2. Electronic health record analysis

Healthcare services on the cloud based on electronic health records (EHRs) analysis are becoming increasingly popular because of their potential to improve patient care and outcomes [27]. By harnessing the power of cloud computing, healthcare providers can efficiently process and analyze large volumes of patient data to gain meaningful insight. These insights can then be used to develop personalized treatment plans and improve overall healthcare delivery.

Gómez *et al.* [28] addressed the issue of EHR system interoperability by selecting several mainstream health informatics standards and applying them to their proposed architectures. The resulting architecture provides a combination of multiple EHR systems and enables scalability through cloud computing capabilities and on-demand modeling of new requirements. The proposal was confirmed through a measurement framework and achieved a high score compared to similar works, demonstrating its effectiveness in terms of EHR system interoperability. Future work will include implementing the proposed architecture and evaluating its performance and efficiency in exchanging information among various EHR systems.

Nguyen *et al.* [29] proposed a new EHRs distribution system that uses wireless cloud computing and blockchain technology. The authors identified and addressed the challenges faced by current EHR sharing systems, particularly those related to access control and data security. They deployed an Ethereum network on an Amazon cloud and used a mobile Android application to allow the healthcare entities to interact with the system. The findings of the implementation demonstrated that the proposed framework provides reliable and fast EHRs sharing with improved privacy and security compared to traditional systems.

Wei *et al.* [30] proposed a new cryptographic primitive called revocable-storage hierarchical attribute-based encryption (RS-HABE) and permission architecture to securely share EHR data in a public cloud. The proposed scheme addresses practical security challenges related to user revocation, keystroke delegation, and ciphertext update. The authors provided a concrete construction of the RS-HABE method that guarantees the advance and reverse security of the encoded EHR data and enables each client to create unique private keys for their children. They demonstrated the security of the scheme using a typical model and provided a theoretical analysis to demonstrate its functionality and security advantages. The recommended RS-HABE method was also implemented and evaluated for its practical performance, demonstrating its effectiveness in securing EHR distribution in public clouds.

Liu *et al.* [31] developed an identity authentication method involving bilinear pairing for personal health record (PHR) systems utilizing cloud computing and sensor networks. The identity authentication mechanism is essential for protecting the privacy and security of users' private data in cloud computing environments. By recording users' daily physical and mental well-being, medical histories, and prescription drug histories, long-term records can be stored on back-end servers for future use. A PHR system and full authentication will not only allow healthcare service providers to verify a user's health status more quickly but also protect their personal privacy and sensitive information. The proposed authentication scheme uses smart cards to store data and verification-required parameters and to secure the entire system.

Rocha and Almeida [32] describe an open-source cloud infrastructure for eHealth analytics that is designed to securely store and exchange the biometric information of volunteers from different sites. The platform collects biometric information and evaluates biometric data, which has the potential to improve the health of older adults who participate in regular fitness exercises. The SaphiraWeb framework is currently a small autonomous system. However, the authors are working to improve it by streamlining data entry from bioelectrical impedance analysis (BIA) devices and integrating it with other compliance domains. This study proposes a standardized approach to e-health analysis that can be applied in different settings.

Kim *et al.* [33] suggest a safe protocol for blockchain-based cloud-assisted EHR systems prevent leakage or falsification of sensitive patient information. The proposed approach has six phases: authorization, registration, EHR storage, smart contract upload, EHR request, and record transaction upload, to ensure secure shared authentication, full anonymity, and complete forward confidentiality. The security of the proposed approach against man-in-the-middle (MITM) and attack replays was demonstrated using the automated validation of internet security protocols and applications (AVISPA) simulations, and the efficiency and security of the scheme were compared with those of related schemes, showing that the proposed approach has greater security and efficiency. The study concludes that the presented EHR system can be applied to real healthcare systems, and suggests creating plausible simulations to evaluate the protocol.

4.3. Health management and prediction

Cloud healthcare services that focus on health management and prediction involve the use of cloud computing to store and process health-related data [34]. These services use advanced analytics and machine learning techniques to monitor and analyze patient data to predict potential health problems and manage patient care. By providing real-time access to patient data, cloud-based health management and prediction services can improve patient outcomes, reduce costs, and streamline healthcare delivery.

Wu *et al.* [35] proposed FedHome, a cloud-edge collaborative learning system for personal health monitoring that protects user privacy by maintaining local data. FedHome trains a global model by aggregating data from numerous houses and then personalizes model learning through knowledge transfer. The proposed framework uses a generative convolutional autoencoder (GCAE) to address the mathematics and communication challenges present in federated training and has demonstrated effectiveness in human activity recognition experiments.

Cao *et al.* [36] discussed the architecture of an IoT system for monitoring medical and health conditions based on cloud computing, which includes gateway terminals, sensor terminals, and an industrial platform. This system allows users to gather personal biological data via medical equipment and transmit them to an underlying healthcare platform system via a portable global system for mobile communication-time division (GSM-TD) communication protocol. The system also allows users to access it using the world wide web/wireless application protocol (WEB/WAP) network. The integration features of the cloud healthcare platform can provide value-added services such as appointment scheduling, maternity and child healthcare, and the sharing of medical data. The system was designed such that it did not reboot or crash during testing.

Cui *et al.* [37] propose a layered architecture for an IoT-based patient health monitoring system, which uses cloud computing to store and evaluate medical data. The system uses related sensors and the IoT devices to track and measure vital signs and to store them in a cloud archive for analysis. The proposed system focuses on rapid data retrieval and is assessed in terms of success, latency, and cost. The overall efficiency of the system was examined using the proportional increase in the reaction time, and the results showed that this system can process medical data efficiently in a fast and reliable manner.

Chakraborty and Kishor [38] demonstrated an internet of medical things-based (IoMT-based) healthcare monitoring system for predicting cardiac diseases and evaluated its performance using various metrics. The proposed model achieved high accuracy, precision, recall, specificity, G-mean, and F1-measure, while consuming very little computational time. It is also superior to previously developed healthcare models. The model can effectively detect patients' cardiac diseases and monitor their heart conditions and can help doctors provide timely treatment depending on the circumstances. Future studies should focus on improving the predictive classifications for the identification of heart disease using attribute selection, novel innovations, and optimization methods.

AlQaheri *et al.* proposed an intelligent monitoring system to identify coronavirus disease 2019 (COVID-19) patients and keep track of them when they are isolated at home. The patients'symptoms were collected using various electronic devices, and the data were transferred to the cloud for analysis [39]. Statistical analysis and fuzzy reasoning were used to inform decisions based on the patients primary signs. The suggested approach was confirmed using real datasets from the World Health Organization (WHO) and Kaggle, achieving an overall recall of 92% and an accuracy of 91%. Future research directions include enhancing the efficiency of the model and increasing data transfer throughput.

4.4. Patient population analysis

Healthcare services on the cloud are based on patient population analysis using cloud computing technology to analyze and manage patient data at the population level [40]. This allows healthcare providers to identify patterns, trends, and potential health risks across different patient populations. By analyzing vast volumes of data such as EHRs, patient demographics, and social determinants of health, these services can help healthcare providers deliver personalized care, improve patient outcomes, and reduce healthcare costs. These services can also enable healthcare providers to make data-driven decisions, improve resource allocation, and plan public health interventions.

Pérez and Salvachúa [41] discuss the need for EHRs to track the activities of older adults in their houses due to the increase in the number of elderly people. However, the current e-health solutions have flexibility, accessibility, and extensibility issues. This study proposes a method for building cloud-based internet of thing-responsive (IoT-Responsive) services for e-healthcare for the elderly at home using architectural patterns, microservices, and the software structure methodology of Rozanski and Woods. The system architecture elements are delivered in a cloud service using the container as a service (CaaS) paradigm, and the microservice deployment is made accessible by DevOps methods using a continuous integration and continuous deployment (CI/CD) pipeline.

The health cloud diagnostic system was developed using machine learning to predict heart diseases [42]. Various models were trained and evaluated for their reliability, precision, crossover validation outcomes, specificity, sensitivity, and area under curve (AUC) scores. The model that performed the best in terms of speed and accuracy was discovered to be logistic regression, and it was used to analyze data in real time on model iPhone operation system (IOS) software hosted on Google Cloud Firebase. The system is designed to offer reliable forecasts and appropriate recommendations to help individuals communicate their symptoms to their doctors and is not intended to replace traditional physical healthcare.

4.5. Security and privacy protection

Cloud healthcare services on security and privacy protection are intended to assure the confidentiality, integrity, and accessibility of patient data stored and processed in the cloud [43], [44]. The increasing adoption of cloud computing in healthcare has created challenges for patient data security and privacy, particularly owing to the sensitive nature of healthcare information. To address these challenges, cloud-based security solutions have been developed, which include data encryption, access control, and audit logging. These solutions are essential for protecting patient data from unauthorized access, data breaches, and cyberattacks. In addition, healthcare services on the cloud also employ privacy-preserving techniques, such as data anonymization and pseudonymization, to protect the privacy of patient data. These techniques enable healthcare providers to share patient data with authorized parties while protecting the patient's identity. Additionally, healthcare services on the cloud use secure communication protocols to warranty encrypted transfer of data between the cloud and healthcare providers.

Hu *et al.* [45] propose a trust-based dynamic authorization paradigm for medical big data. The model calculates the global trust values of participating parties to quantify trust and adds a dual-way choosing mechanism and a 3rd-party monitoring procedure to provide real-time access control. Simulations and comparative experiments show that the model provides good improvements with regard to trust accuracy, dynamic controllability, time complexity, and environmental adaptability. However, the performance of the model in complex and changing real-world environments remains to be tested. Future work will concentrate on establishing a practical evaluation metric framework to reduce the time complexity of the model.

Kanwal *et al.* [46] addressed the challenge of providing privacy-aware authorized access to EHRs in a cloud-based hybrid environment. The authors created a taxonomy of privacy methods in cloud-based EHRs, categorizing them into data encryption, cryptographic authentication, and security-aware anonymization-based approaches. They analyzed various preserving privacy options for cloud-based EHRs and proposed a security-aware authentication model that combines eXtensible access control markup language (XACML) attribute-based authentication with the confidentiality method Angel to outsource EHRs data to cloud environments. The privacy-preserving XACML based access control (PPX-AC) hypothesis offers fine-grained authentication and validates it against both internal and external privacy attacks. The testing results demonstrate the effectiveness of the prototype as it relates to the authentication performance settings inside the PPX-AC paradigm.

Kong *et al.* [47] proposed a S-AlexNet convolutional neural network and dynamic game theory (SCNN-DGT) model to evaluate service providers' reputations for health information safety in a cloud setting. The model is built on a dynamic game design and recommendation incentive strategy and uses convolutional neural network training to determine users' reputation for the security of their health data. The SCNN-DGT model addresses the issue of conveying the credibility value of service suppliers through a trustworthy recommendation standing evaluation structure and incentive technique. The experimental results show that the SCNN-DGT model beats the existing approaches in terms of accurate information recognizing rate, convergence speed, and recommendation effectiveness. Future research directions include optimizing the learning capability of convolution neural networks and game theory to respond more dynamically to dynamic changes.

Kanwal *et al.* [48] discussed the need for privacy-preserving techniques for EHRs stored in the cloud environment and provided a comprehensive analysis of various privacy techniques and their applicability to different types of data. The authors identified the need for a combination of privacy techniques and models to improve the privacy and utility of published data and proposed a taxonomy of specific privacy requirements for EHRs. This study also includes an analysis of privacy techniques in light of the requirements of the general data protection regulation (GDPR) in the European Union (EU).

Yadav *et al.* [49] proposed a secure e-health system that allows the secure collaboration of EHRs in the cloud. The system is more effective and performs better than existing systems while meeting all the necessary privacy requirements. The system is suitable for resource-constrained devices on the internet of medical things (IoMT). However, if the public cloud is a centralized secure cloud, the system is subject to a single point of breakdown.

Rajasekar *et al*. [50] provided a systematic review of recent advances in remote user authentication schemes grouped into three layers: healthcare applications, the IoT applications, and cloud/multi-server applications. The need for mutual authentication between cloud service providers and mobile users is highlighted, with approximately 100 recent remote user authentication schemes analyzed and compared in terms of various performance parameters. The ongoing research in this area is expected to be useful in identifying desirable attributes and outlining security attacks in emerging real-time applications. Future research should focus on areas such as agriculture, e-governance, smart cities, and e-passport.

Chenthara *et al.* [51] discussed the need to protect smart healthcare services from unauthorized access and highlighted the vulnerabilities of the existing solutions. Because much of the data are stored on cloud servers, they are extremely vulnerable to attacks and hacking. This review offers a thorough analysis of current e-health cloud-preserving encrypted and non-encrypted strategies to protect privacy in the cloud environment, and identifies key research areas, remarkable research challenges, and potential study directions to guarantee impenetrable privacy in smart healthcare responses. The evolution of holistic security mechanisms can make healthcare data more secure and sustainable.

5. CONCLUSION AND LIMITATIONS

This review provides a comprehensive overview of healthcare services on cloud services and previous studies in this area. Using the PRISMA process methodology, we conducted an extensive search of the Web of Science database for journal articles published within the last five years, resulting in the selection of 23 papers. Through clustering analysis of the selected papers, we identified the five most frequent application scenarios for healthcare services in the cloud environment. Based on an in-depth study of the literature, we identify several key factors for evaluating such services, including security and privacy, user cost, accuracy, operability, scalability, access control, interoperability, reliability, robustness, computational cost, and throughput. However, the current research is limited to only a few of these factors, and there is a lack of a unified platform or framework to balance all the factors comprehensively and equitably. Our findings suggest that a unified framework for healthcare services in the cloud environment can be developed by leveraging the benefits of cloud computing in storing and processing large volumes of data and integrating data encryption and hybrid access control mechanisms. To extend healthcare services to a wider range of application scenarios, future research should consider emerging trends and unresolved issues, such as healthcare resource optimization, online consultation, patient population analysis, clinical trial design, health insurance claims, and drug development.

However, there are certain limitations to our review. First, our article was only initially researched using the following keywords: “cloud-based healthcare facilities, cloud-based healthcare services, and cloud-based healthcare facilities.” Second, our search was limited to the Web of Science online database, which may not have provided a comprehensive overview of the topic. Additionally, many other publishers and journals can provide a more comprehensive understanding of healthcare services in the cloud. Finally, our review excluded publications written in non-English languages, even though some research on healthcare services in the cloud is being conducted and published in different languages.

6. FUTURE RESEARCH DIRECTIONS

Several research directions for healthcare services in the cloud environment can be pursued in the future. First, more empirical studies are required to assess the impact and efficiency of these services in improving patient outcomes, reducing costs, and increasing the effectiveness and efficiency of healthcare services. This may involve conducting randomized controlled trials or longitudinal studies to assess the impact of cloud-based healthcare services on various health outcomes. Second, there is a need to investigate the ethical and legal implications of healthcare services in the cloud, particularly with regard to patient data privacy and security. This may involve exploring regulatory frameworks governing cloud-based healthcare services and identifying the best practices for protecting patient data in cloud environments. Third, innovative technologies like the IoT and artificial intelligence (AI), should be explored to enhance healthcare services in the cloud. This may involve investigating how these technologies can be integrated into existing cloud-based healthcare platforms to improve care delivery and patient outcome. Finally, there is a need for research on the adoption and implementation of healthcare services in the cloud, particularly in low resource settings. This may involve exploring the barriers and facilitators of acceptance of healthcare services in cloud environments in different healthcare settings and identifying strategies to overcome these barriers.

REFERENCES

[1] S. H. Talib, L. A. Abdul-Rahaim, A. J. Alrubaie, and I. M. Raseed, "Design smart hospital system based on cloud computing," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 29, no. 2, pp. 797–807, Feb. 2023, doi: 10.11591/ijeecs.v29.i2.pp797-807.

[2] I. Ahmed, "Technology organization environment framework in cloud computing," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 2, pp. 716–725, Apr. 2020, doi: 10.12928/telkomnika.v18i2.13871.

[3] J. H. Majeed and Q. Aish, "A remote patient monitoring based on WBAN implementation with internet of thing and cloud server," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 3, pp. 1640–1647, Jun. 2021, doi: 10.11591/eei.v10i3.1813.

[4] H. A. Abdulmalek and A. A. Yassin, "Secure two-factor mutual authentication scheme using shared image in medical healthcare environment," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 4, pp. 2474–2483, Aug. 2023, doi: 10.11591/eei.v12i4.4459.

[5] B. Wu, F. Tian, M. Zhang, H. Zeng, and Y. Zeng, "Cloud services with big data provide a solution for monitoring and tracking sustainable development goals," *Geography and Sustainability*, vol. 1, no. 1, pp. 25–32, Mar. 2020, doi: 10.1016/j.geosus.2020.03.006.

[6] A. Bhawiyuga, S. A. Kharisma, B. J. Santoso, D. P. Kartikasari, and A. P. Kirana, "Cloud-based middleware for supporting batch and stream access over smart healthcare wearable device," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 5, pp. 1990–1997, Oct. 2020, doi: 10.11591/eei.v9i5.1978.

[7] F. Abdali-Mohammadi, M. N. Meqdad, and S. Kadry, "Development of an IoT-based and cloud-based disease prediction and diagnosis system for healthcare using machine learning algorithms," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 9, no. 4, pp. 766–771, Dec. 2020, doi: 10.11591/ijai.v9.i4.pp766-771.

[8] O. A. Wahab, R. Cohen, J. Bentahar, H. Otrok, A. Mourad, and G. Rjoub, "An endorsement-based trust bootstrapping approach for newcomer cloud services," *Information Sciences*, vol. 527, pp. 159–175, Jul. 2020, doi: 10.1016/j.ins.2020.03.102.

[9] S. M. Rukmony and S. Gnanamony, "Rough set method-cloud internet of things: a two-degree verification scheme for security in cloud-internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 2233–2239, Apr. 2023, doi: 10.11591/ijece.v13i2.pp2233-2239.

[10] M. Usak, M. Kubiatko, M. S. Shabbir, O. V. Dudnik, K. Jermsittiparsert, and L. Rajabion, "Health care service delivery based on the Internet of things: A systematic and comprehensive study," *International Journal of Communication Systems*, vol. 33, no. 2, Jan. 2020, doi: 10.1002/dac.4179.

[11] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, "A robust and lightweight secure access scheme for cloud based E-healthcare services," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3043–3057, Sep. 2021, doi: 10.1007/s12083-021-01162-x.

[12] F. Ali *et al.*, "An intelligent healthcare monitoring framework using wearable sensors and social networking data," *Future Generation Computer Systems*, vol. 114, pp. 23–43, Jan. 2021, doi: 10.1016/j.future.2020.07.047.

[13] J. M. Puaschunder, "The potential for artificial intelligence in healthcare," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3525037.

[14] B. Pourghebleh, V. Hayyolalam, and A. Aghaei Anvigh, "Service discovery in the internet of things: review of current trends and research challenges," *Wireless Networks*, vol. 26, no. 7, pp. 5371–5391, Oct. 2020, doi: 10.1007/s11276-020-02405-0.

[15] B. L. Putro, Y. Rosmansyah, and S. Suhardi, "An intelligent agent model for learning group development in the digital learning environment: A systematic literature review," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 3, pp. 1159–1166, Jun. 2020, doi: 10.11591/eei.v9i3.2009.

[16] M. Rahimi, N. J. Navimipour, M. Hosseinzadeh, M. H. Moattar, and A. Darwesh, "Toward the efficient service selection approaches in cloud computing," *Kybernetes*, vol. 51, no. 4, pp. 1388–1412, Mar. 2022, doi: 10.1108/K-02-2021-0129.

[17] A. Heidari and N. J. Navimipour, "Service discovery mechanisms in cloud computing: a comprehensive and systematic literature review," *Kybernetes*, vol. 51, no. 3, pp. 952–981, Feb. 2022, doi: 10.1108/K-12-2020-0909.

[18] S. Vahdat and S. Shahidi, "D-dimer levels in chronic kidney illness: A comprehensive and systematic literature review," *Proceedings of the National Academy of Sciences, India Section B: Biological Sciences*, vol. 90, no. 5, pp. 911–928, Dec. 2020, doi: 10.1007/s40011-020-01172-4.

[19] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Computers in Industry*, vol. 122, Nov. 2020, doi: 10.1016/j.compind.2020.103290.

[20] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *International Journal of Information Management*, vol. 43, pp. 146–158, Dec. 2018, doi: 10.1016/j.ijinfomgt.2018.07.009.

[21] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: A survey," *Journal of Healthcare Engineering*, vol. 2019, pp. 1–15, Sep. 2019, doi: 10.1155/2019/7516035.

[22] A. Sahi, D. Lai, and Y. Li, “A review of the state of the art in privacy and security in the eHealth cloud,” *IEEE Access*, vol. 9, pp. 104127–104141, 2021, doi: 10.1109/ACCESS.2021.3098708.
[23] M. R. Ahmed, S. M. H. Mahmud, M. A. Hossin, H. Jahan, and S. R. H. Noori, “A cloud based four-tier architecture for early detection of heart disease with machine learning algorithms,” in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, Dec. 2018, pp. 1951–1955, doi: 10.1109/CompComm.2018.8781022.
[24] A. Alourani, K. Tariq, M. Tahir, and M. Sardaraz, “Patient mortality prediction and analysis of health cloud data using a deep neural network,” *Applied Sciences*, vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042391.
[25] K. Sreelatha and V. K. Reddy, “Integrity and memory consumption aware electronic health record handling in cloud,” *Concurrent Engineering*, vol. 29, no. 3, pp. 258–265, Sep. 2021, doi: 10.1177/1063293X211027869.
[26] X. Zhu, J. Shi, and C. Lu, “Cloud health resource sharing based on consensus-oriented blockchain technology: case study on a breast tumor diagnosis service,” *Journal of Medical Internet Research*, vol. 21, no. 7, Jul. 2019, doi: 10.2196/13767.
[27] M. Tayefi *et al.*, “Challenges and opportunities beyond structured data in analysis of electronic health records,” *WIREs Computational Statistics*, vol. 13, no. 6, Nov. 2021, doi: 10.1002/wics.1549.
[28] D. Gómez *et al.*, “Cloud architecture for electronic health record systems interoperability,” *Technology and Health Care*, vol. 30, no. 3, pp. 551–564, May 2022, doi: 10.3233/THC-212806.
[29] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for secure EHRs sharing of mobile cloud based e-health systems,” *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.
[30] J. Wei, X. Chen, X. Huang, X. Hu, and W. Susilo, “RS-HABE: revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud,” *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2019, doi: 10.1109/TDSC.2019.2947920.
[31] C.-H. Liu, T.-L. Chen, C.-Y. Chang, and Z.-Y. Wu, “A reliable authentication scheme of personal health records in cloud computing,” *Wireless Networks*, Aug. 2021, doi: 10.1007/s11276-021-02743-7.
[32] L. A. Rocha and S. S. Almeida, “Saphiraweb: An open-source cloud platform for E-health analysis,” *Instrumentation Science and Technology*, vol. 48, no. 6, pp. 583–600, Nov. 2020, doi: 10.1080/10739149.2020.1761380.
[33] 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, May 2020, doi: 10.3390/s20102913.
[34] S. Tabassum, M. Sampa, R. Maruf, F. Yokota, N. Nakashima, and A. Ahmed, “An analysis on remote healthcare data for future health risk prediction to reduce health management cost,” *APAMI 2020c: 11th Biennial Conference of the Asia-Pacific Association for Medical Informatics*, vol. 115–119, 2020.
[35] Q. Wu, X. Chen, Z. Zhou, and J. Zhang, “FedHome: cloud-edge based personalized federated learning for in-home health monitoring,” *IEEE Transactions on Mobile Computing*, vol. 21, no. 8, pp. 2818–2832, Aug. 2022, doi: 10.1109/TMC.2020.3045266.
[36] S. Cao *et al.*, “Cloud computing-based medical health monitoring IoT system design,” *Mobile Information Systems*, vol. 2021, pp. 1–12, Jul. 2021, doi: 10.1155/2021/8278612.
[37] M. Cui, S.-S. Baek, R. G. Crespo, and R. Premalatha, “Internet of things-based cloud computing platform for analyzing the physical health condition,” *Technology and Health Care*, vol. 29, no. 6, pp. 1233–1247, Nov. 2021, doi: 10.3233/THC-213003.
[38] C. Chakraborty and A. Kishor, “Real-time cloud-based patient-centric monitoring using computational health systems,” *IEEE Transactions on Computational Social Systems*, vol. 9, no. 6, pp. 1613–1623, Dec. 2022, doi: 10.1109/TCSS.2022.3170375.
[39] H. AlQaheri, M. Sarkar, S. Gupta, and B. Gaur, “Intelligent cloud IoMT health monitoring-based system for COVID-19,” *Computers, Materials and Continua*, vol. 72, no. 1, pp. 497–517, 2022, doi: 10.32604/cmc.2022.022735.
[40] J. H. Y. Ng and B. H. K. Luk, “Patient satisfaction: Concept analysis in the healthcare context,” *Patient Education and Counseling*, vol. 102, no. 4, pp. 790–796, Apr. 2019, doi: 10.1016/j.pec.2018.11.013.
[41] L. Jurado Pérez and J. Salvachúa, “An approach to build e-health IoT reactive multi-services based on technologies around cloud computing for elderly care in smart city homes,” *Applied Sciences*, vol. 11, no. 11, Jun. 2021, doi: 10.3390/app11115172.
[42] F. Desai *et al.*, “HealthCloud: A system for monitoring health status of heart patients using machine learning and cloud computing,” *Internet of Things*, vol. 17, Mar. 2022, doi: 10.1016/j.iot.2021.100485.
[43] H. X. Son, M. H. Nguyen, H. K. Vo, and T. P. Nguyen, “Toward an privacy protection based on access control model in hybrid cloud for healthcare systems,” in *Advances in Intelligent Systems and Computing*, Springer International Publishing, 2020, pp. 77–86.
[44] R. Sivan and Z. A. Zukarnain, “Security and privacy in cloud-based e-health system,” *Symmetry*, vol. 13, no. 5, Apr. 2021, doi: 10.3390/sym13050742.
[45] X. Hu, R. Jiang, M. Shi, and J. Shang, “A privacy protection model for health care big data based on trust evaluation access control in cloud service environment,” *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 3, pp. 3167–3178, Mar. 2020, doi: 10.3233/JIFS-191149.
[46] T. Kanwal, A. Anjum, S. U. R. Malik, A. Khan, and M. A. Khan, “Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud,” *Computer Standards and Interfaces*, vol. 78, Oct. 2021, doi: 10.1016/j.csi.2021.103522.
[47] F. Kong, Y. Zhou, B. Xia, L. Pan, and L. Zhu, “A security reputation model for IoT health data using S-AlexNet and dynamic game theory in cloud computing environment,” *IEEE Access*, vol. 7, pp. 161822–161830, 2019, doi: 10.1109/ACCESS.2019.2950731.
[48] T. Kanwal, A. Anjum, and A. Khan, “Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities,” *Cluster Computing*, vol. 24, no. 1, pp. 293–317, Mar. 2021, doi: 10.1007/s10586-020-03106-1.
[49] V. K. Yadav, R. K. Yadav, S. Verma, and S. Venkatesan, “CP2EH: a comprehensive privacy-preserving e-health scheme over cloud,” *The Journal of Supercomputing*, vol. 78, no. 2, pp. 2386–2416, Feb. 2022, doi: 10.1007/s11227-021-03967-2.
[50] V. Rajasekar, P. Jayapaul, S. Krishnamoorthi, and M. Saračević, “Secure remote user authentication scheme on health care, IoT and cloud applications: a multilayer systematic survey,” *Acta Polytechnica Hungarica*, vol. 18, no. 3, pp. 87–106, 2021, doi: 10.12700/APH.18.3.2021.3.5.
[51] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and privacy-preserving challenges of e-Health solutions in cloud computing,” *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

BIOGRAPHIES OF AUTHORS

Bo Guo is currently pursuing a Ph.D. in computer science at Universiti Selangor in Malaysia and is also teaching at the School of Computer and Information Engineering, Fuyang Normal University, Fuyang City, China. His research interests include data mining, image processing, pattern recognition, big data, and so on. He can be contacted at email: 9212000331@istudent.unisel.edu.my.

Nur Syufiza Ahmad Shukor has seven years of industry experience in systems development before joining UNISEL in 2003, where she was involved in several IT projects and also played important roles (team leader and project manager) in application development projects. She started her academic career in 1998 as an IT part-time lecturer at a private college. Her experience in the industry along with her passion for academic work brought her to several administrative positions in the faculty (as Head of Program and Deputy Dean (Academic)) before earning her Ph.D. in information systems at Universiti Teknologi Malaysia. She served as one of the Business Architect for in-house Total Campus Management Systems for more than two years at her university before she was once again assigned managerial post as the Director of the International Office. She is now the Director of the Centers of Research Excellence UNISEL. Her current interests include knowledge management, knowledge audit, inter-organizational knowledge sharing and collaboration between organizations, digital citizens, ICT4D, ICT governance, and big data analytics. She can be contacted at email: nur_syufiza@unisel.edu.my.

Irny Suzila Ishak is a senior lecturer at Universiti Selangor in Malaysia. Her research interests are in the areas of strategic ICT planning, strategic planning, ICT innovation, ICT implementation, ICT benchmarking, big data analytics, and IoT. Her research group focuses on how IoT and big data mobile applications and web-based systems can help the community. Her current research focus is on how ICT can help in aquaculture, the tourism industry, community health, community sustainability, and children's education. Her postgraduate research titles are "Designing strategic information systems planning methodology for Malaysian IHLs" and "Strategic ICT planning methodology to promote innovation in organizations". She can be contacted at email: irny@unisel.edu.my.