International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

TRANSFORMATIVE IMPACT OF CLOUD COMPUTING ON HUMAN HEALTH CARE

Manisha Divate and Aaswat Vishwakarma
Usha Pravin Gandhi College of Arts, Science and Commerce

ABSTRACT
In the Healthcare Industry cloud computing is being adopted and integrated into their systems by analysing its transformative effects, opportunities and challenges and its future in the healthcare sector. This shows how traditional hospitals used to store data in their drives and how it has transitioned into digital data because of the cloud. Because it has improved scalability, collaboration and cost-effectiveness, in this, we delve into cloud computing influences in the healthcare sector.

It shows its potential in telemedicine and private healthcare and the potential security risks and data privacy concerns. Regardless of concerns, cloud computing in the healthcare sector plays an important part in improving the state of healthcare and making critical decisions for the patient's treatment.

Keywords: Cloud Computing, Healthcare, Health, Security, Challenges, Services.

1. INTRODUCTION
Indian hospitals including Tata Memorial, Kokilaben Dhirubhai Ambani, and AIIMS used outdated data storage methods before online computing became common. These platforms involved using servers on- premises and had limits concerning accessibility and scalability. Infrastructure limitations have limited the accessibility of services related to telemedicine. The Local methods were the only means to guarantee data security, and protecting it costs a lot of money. Following these organizations have transition to cloud- based storage, which improved scalability, made telemedicine collaboration easy, implemented advanced security features, and significantly reduced infrastructure costs. This completely changed the way healthcare operated, improving the treatment of patients, making data more accessible, and promoting technological innovation.

Cloud computing means the usage of cloud-based resources such as storage of data, networking, databases, servers, and computer programs over an internet connection. All the information is kept on server hardware maintained by a company that provides cloud services. In the case of cloud computing, the capabilities of computers, including the storage of data and the ability to compute, can be provided in demand while avoiding supervision by the individual who uses them. Infrastructure as a service, also known as (IaaS), platform as a service (PaaS), and software as a service (SaaS). comprise some of the services it provides. Infrastructure as a Service offers virtual resources like storage space and systems, whereas users may share resources and expand their computer system capability according to their requirements with IaaS.

A few of the major IaaS suppliers include Juniper Networks, IBM, VMware, and Amazon, for example. PaaS supports program creation and execution, and PaaS supports web user interface scaling, database integration, teamwork, and subscription and payment management for applications produced. Google, IBM, and Oracle are a few PaaS vendors. and SaaS provides software programs via subscriptions. SaaS is appropriate for a variety of applications, including Oracle, SAP, Salesforce and salesforce.com, and provides integration across disparate software components. SaaS suppliers include companies like IBM, Salesforce, and Google. [31].

Public, private, hybrid, and community clouds are all types of cloud setups. Public clouds are accessible to all consumers, whereas private clouds provide a unique architecture for one organization, hybrid clouds combine public and private capabilities, and community clouds fulfil the requirements of several organizations.

Understanding these models could assist companies in adjusting their cloud-based approach depending on their own functioning, security, and sustainability needs.

2. SYSTEMATIC REVIEW:
. To broaden the scope of our studied literature, methodology, and review articles, we began to recognize some of the most often-used substitute words/concepts and counterparts in the study and review papers.

Cloud Computing, cloud, Healthcare, Health, Cloud- Security, Challenges, Services, Techniques, security, (eHealth OR "electronic health")

We first searched for different research papers and review papers and in the end, we got 40 articles, websites research papers and review papers. To focus on the most relevant literature, methodology applications, and

ISSN 2394 - 7780

challenges We did a primary review by reading the introductions of each selected publication. The assessment is founded on the standards outlined in Table 1.

Table 1: Required category

Required category
• Linking eHealth with cloud technologies, either explicitly or implicitly.
• Establish cloud-based eHealth platforms.
• Cloud-based computing methods in healthcare.
• Ensuring medical confidentiality and safety of information in the cloud.
Challenges faced by the healthcare sector.
The Future trends in the healthcare sector.
Different techniques in the cloud.

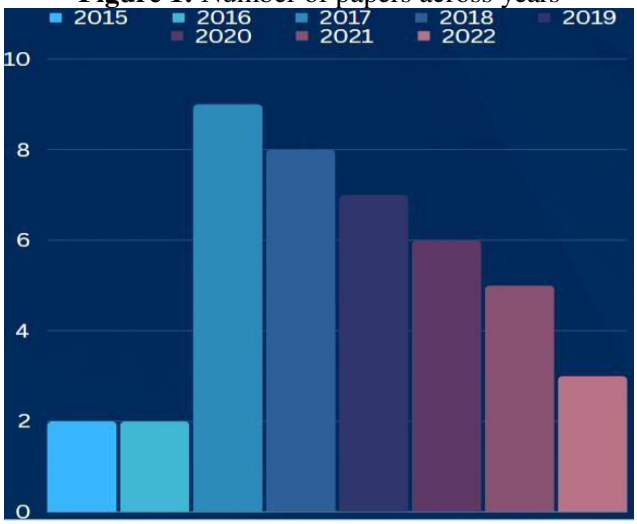
RESULTS

After the steps of searching many different articles, research papers, review papers, and websites, 40 papers and articles were finally selected from the Internet.

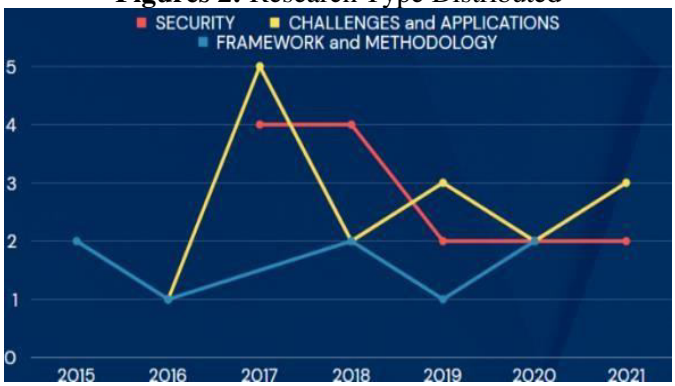
We believe that the selected 40 papers are the perfect view of computing in the healthcare sector and e-health. Both e-health and cloud computing in the healthcare sector are rising exponentially.

Figures 1 and 2 show the research, review papers used in the research, the years they were published, and the category of papers.

Figure 1: Number of papers across years



Figures 2: Research Type Distributed



3. LITERATURE-REVIEW

The use of cloud computing in healthcare systems has received considerable interest due to its ability to change the field. Mohit et al. (2017) researched the use of cloudlet technology in complementing healthcare services using mobile cloud computing. The study aims to improve healthcare app efficiency and accessibility by exploiting cloudlet proximity and resources, highlighting the potential of cloudlets in overcoming mobile device processing restrictions [10]. Another critical element discussed in the literature is the shift to services that are cloud-based in healthcare. A thorough analysis by several writers stressed variables critical for

ISSN 2394 - 7780

effective adoption. This encompassed safety, capacity, pricing, integration, and regulatory compliance, giving organizations insights into how to leverage cloud advantages while limiting concerns [2]. The influence of cloud technology on the efficiency and accessibility of healthcare has been a focus. Cloud computing has many advantages as it can give online data storage capability, information can be shared by interchange among healthcare providers using the data storage, and enhanced patient access to health records, according to research. Furthermore, it addressed security and privacy concerns, emphasizing the importance of strong security measures in cloud [3]. The vast potential of cloud computing in healthcare services has received much attention. Studies have looked into its ability to increase efficiency and sustainability, as well as the hazards linked with it. Various applications, such as telemedicine, data analysis, and tailored healthcare, were investigated, demonstrating the technology's significant impact on the sector [4,40]. Furthermore, the significance of fog computing in Healthcare 4.0 has been examined for its potential to increase productivity and reduce delays. The research emphasized its capacity to provide fast data analysis, secure communication, and improved resource use, resulting in improved patient care and operational flexibility [5]. The integration of cloud-based computer technologies (such as online data storage servers, 24/7 accessible storage, and real-time data regarding certain medical information and the history of patients) because of cloud usage inside healthcare organizations has been praised for its potential to transform patient care. The connection sought to improve data accessibility, real- time patient tracking, and the ability to make quick decisions and provide personalized treatment. In this integration, the study identified both possibilities and obstacles [6]. The integration of IoT and cloud computing in healthcare has also been investigated for its transformational potential. The study clarified their function in patient monitoring and resource management, as well as privacy and scalability problems, providing insights into prospective improvements and obstacles [7]. Furthermore, the disruptive influence of cloud computing on IT systems and service delivery paradigms was examined, with a focus on its capacity, mobility, and cost-effectiveness in enhancing operations. [8]. The research has discussed the potential hazards which are associated with the adoption of cloud computing in the healthcare sector it highlights the vulnerabilities to security attacks, access control, and identity identification There are also risks such as malware attacks, data corruption, data loss, and unauthorized access [9].

Mohit et al. (2017) found a focus on secure methods of authentication powered by cloud healthcare systems. The report emphasized the need for strong authentication mechanisms in protecting patient information, as well as the need for particular safety precautions stored in the cloud healthcare administration [10].

In the summary of the literature review, the research paper by Alam "Cloud Computing and its Role in Information Technology" (2021) addresses the significance of cloud computing in several industries, including healthcare, and underlines its potential benefits and limitations in the article. The study also discusses the probable future of computing in the cloud's impact on healthcare enterprises. it also emphasizes the significance of online computing in streamlining procedures, reducing paperwork, and safeguarding patient data. The study does, however, highlight significant problems, such as the danger of data leaks and the necessity for cautious execution to achieve favourable results. [8].

4. METHODOLOGY

Srivastava and Khan's 2018 review on cloud computing probably employed a sophisticated analytical approach. It likely encompassed comprehensive literature analysis, meta-analyses, experiments, simulations, surveys, classification methodologies, and intricate survey techniques. To substantiate their findings, the researchers might have utilized both quantitative and qualitative studies. The study has emphasized resource allocation strategies, scheduling approaches, load management techniques, and admission control methods within the domain of cloud computing. These methodological facets likely ensured a meticulous, rigorous, and comprehensive exploration of contemporary research and developments in cloud computing. [11]. In "Using Cloud Computing Services in the E-learning Process Has Its Benefits and Challenges," The researchers have reviewed the existing literature to give a comprehensive assessment of the advantages and disadvantages of employing cloud-based technology in e-learning. Their method included examining multiple academic papers to define the existing environment and the impact of the cloud on online education. The researcher tackled the basic principles of online education and the use of cloud computing technology while addressing the benefits and drawbacks of their combination. Furthermore, the researchers investigated cloud-centric e-learning products and discussed common concerns found while installing online e-learning systems, providing effective solutions for these obstacles.[12]. "Safety and safeguards difficulties with e-health services methods" by Sadoughi et al. (2019) investigated and defined significant safety and privacy difficulties related to e-health solutions in the context of cloud computing through a comprehensive study of the literature and quantitative synthesis approaches. Some of the techniques and methods used in this paper are:

ISSN 2394 - 7780

1. **cryptographic security**: Public Key Encryption (PKE) and Symmetric Key Encryption, (SKE) Broadcast Encryption Programs, Qualified Encryption, Block Chain-Based Encryption, Searchable Symmetric Encryption,
2. **Access control Manager(ACM),**
3. **Identity-Based Encryption**

[13]. Jin and Chen (2015) used a variety of approaches to evaluate the opportunities and difficulties of telemedicine in the cloud. Their methodology involved analysing documents and a review of many telemedicine and cloud-based computing papers and research they have used methods such as Picture Archiving and communication systems, Telemonitoring biosignal processers, and Multimedia medical consultations in these papers but there are also challenges for telemedicine in cloud computing which are data interoperability, privacy and authentication, system security regulatory issues [14]. a thorough examination of cloud computing-related data security issues and their resolutions. There are various methods and techniques by the author in the papers which has been discussed to ensure data security in cloud computing. These include Identity and Access Management (IAM), Encryption, Virtual Private Networks (VPNs), Compliance and risk management, User activity monitoring, Regular audits and policy establishment, Ongoing training for staff to combat emerging threats, Backing up data, Implementing access management controls at the file and field levels, Identifying storage locations for structured and unstructured data and Implementing encryption for data in transit and data at rest.

This paper's methodology evaluation illustrates a thorough and methodical approach to examining cloud computing data security resolutions in cloud computing. [15].

Data security is a significant responsibility of both healthcare providers and patients. Organizations may reduce the serious hazards associated with non-cloud data storage techniques by using a cloud-based approach by recognising and eliminating any current vulnerabilities, cloud computing systems can safeguard from possible risks. By complying with HIPAA guidelines, cloud techniques can further improve the security of data**.**

To critically analyse the application of big data analysis in healthcare, evaluate the current literature and highlight major concerns with the organization of data, data collecting, preserving data, processing of information, and data display. The researcher has used techniques to analyse the healthcare big data which includes Machine Learning: this is used in analysing big data in healthcare domains, Artificial Intelligence and Data mining which allows the large number of databases from thousands of patients and clients to identify correlations between datasets, and develop models for the medical sector, the researcher examining the possible applications of analytics for big data in the healthcare industry, including managing the health of a population, illness forecast and avoidance, and customized therapy. [16]. Cloud computing has improved data analysis, and machine learning enables healthcare professionals to look for discoveries and patterns in massive amounts of data. This enables improved disease outbreak modelling, personalized treatment and the identification of high-risk patients, ultimately leading to better prevention and treatment methods and outcomes. A quantitative technique is used in the study article to examine the variables influencing the Development of cloud computing services in healthcare. To assess the competency and willingness of departments dealing with IT with different hospitals to adopt cloud computing the research sends questionnaires to these departments. Multiple regression analysis is employed to ascertain the influence of technical, administrative, and environmental variables on the adoption of cloud computing. The research findings have significant importance for ICT managers and providers, and they may aid in developing strategies for the use of cloud- based computing within the healthcare industry.[17] The researcher of "Security Enhancement in Healthcare Cloud using Machine Learning" presents a novel approach that improves the safety of data in cloud settings by utilizing the use of machine learning techniques. The researchers have proposed a cloud framework which consists of two elements to deal with security problems they have used: CloudSec component which first encrypts all health data using HTTPS/SSL protocol to secure data transfer. this module uses a segmentation approach to keep medical images safe and secure. Once encrypted, CloudSec sends clients' data to an external cloud service provider to process them securely, this module is responsible for ensuring privacy and security for clients' data during the utilization of cloud resources. They have used a method that uses both classification and regression by using machine learning theory. this technique uses linear classifiers to evaluate data and identify patterns. it relies heavily on statistical learning theory developed to maximize predictive accuracy. Additionally, when incorporating machine learning technologies inside the healthcare industry, the search results highlight the crucial elements of data quality control, guaranteeing security and confidentiality of information, encouraging cooperation, and ongoing improvement. [18]. The researchers highlight a proposed strategy targeted at giving predictions as well as

ISSN 2394 - 7780

knowledge to hospital administration to get around organizational hurdles during the adoption of big data technologies. Furthermore, the study investigates the possibility of Using vast volumes of data to efficiently solve healthcare problems, such as optimizing treatment paths and improving healthcare systems. The study's findings show that widespread data acceptance, implementation, and usage in healthcare settings might provide considerable advantages and possibilities. [19]. The research suggests a system that utilizes the cloud for handling healthcare data, using biometric identification to ensure safety. The research's approach involves an investigation of a hospital in an underdeveloped nation to guide the creation of the BAMHealthCloud structure, the installation of a fingerprint-based authorization operator for safe data entry and administration, and distributed instruction via the use of the Hadoop MapReduce structure for quicker medical information handling. They have proposed methods such as authentication access to ensure that the legit personnel can access the data stored in a healthcare cloud server, the researcher has proposed 2 methods which are Phase 1 and Phase 2, Phase 1 consists of the staff and the patients in the health care centre and then are asked to enrol themselves by giving their signature samples using either the signature device or their smartphones that are installed with the signature gathering software. Once a user's signature has been taken, the quality of the given signature is checked using SigQuality checker software. The function of this software is to ensure that the recorded signature samples match up to the quality standards required for authentication. Phase 2 consists of the authentication phase which uses an algorithm that takes the user's signature scans it and stores it in the cloud which then can be used to check the authentication of the personnel if they try to access the database and then they are only allowed to use the database if they are given the authentication of it. After these personnel can access the information from the cloud [20]. The researchers used a thematic approach to see the opportunities and benefits of telemedicine in the healthcare sector by having cloud-computing integration, they also showed the techniques used in the study which are IAAS, PAAS, and SAAS [38,39] by using techniques like biometric authentication in distributed data storage systems it provided safe access to the medical personals and hospitals and it ensures the safety of data [39]

The paper "BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in the Cloud" by Shakil, K. A., Zareen,

F. J., Alam, M., and Jabin, S. (2020) introduces a creative approach to addressing the problems associated with medical safety and information administration. The paper's suggested BAMHealthCloud system uses biometric authorization and data storage in the cloud to offer safe access, retrieval, and manipulation of healthcare information. Particularly, the use of distributed learning using the Apache Hadoop MapReduce architecture indicates a smart technological approach that improves the effectiveness of the system.

These approaches show great potential for medical technology because they efficiently handle crucial safety and information management problems in an era of rising digitalization and data transmission within healthcare [20].

5. DISCUSSION AND RESULT:

The healthcare industry has undergone a substantial transition, owing primarily to the introduction and integration of Cloud technology, massive data statistical analysis, machine learning, and advanced technical solutions. Multiple research investigations have highlighted these technologies' enormous potential and different uses in healthcare settings. Mohit et al. (2017) examined the use of cloudlet technologies for boosting medical services. using mobile cloud computing, to improve healthcare app efficiency and accessibility. Furthermore, the move to cloud-based services in healthcare has been highlighted in the literature, emphasizing essential elements for effective adoption such as safety, capacity, cost, and integration.

The importance of cloud computing on healthcare efficiency and accessibility has been highlighted, with cloud computing boosting data storage, information interchange across providers, and increased patient access to health records.

Furthermore, a considerable lot of research has been undertaken on the potential advantages of cloud-based computing in enhancing healthcare performance and sustainable development, as well as its uses in telemedicine, which is an analysis of data, and personalized medical care, indicating major implications on the industry. Fog computing has also received interest in Healthcare 4.0 because of its ability to increase productivity, minimize delays, provide quick data analysis, secure communication, and optimize resource usage, ultimately improving the treatment of patients and flexibility in operations. A cloud-based integration of technology in medical organizations has been recognized for its ability to change the way patients are treated by enhancing access to information, real- time patient monitoring, allowing rapid decision-making processes, and individualized therapy.

ISSN 2394 - 7780

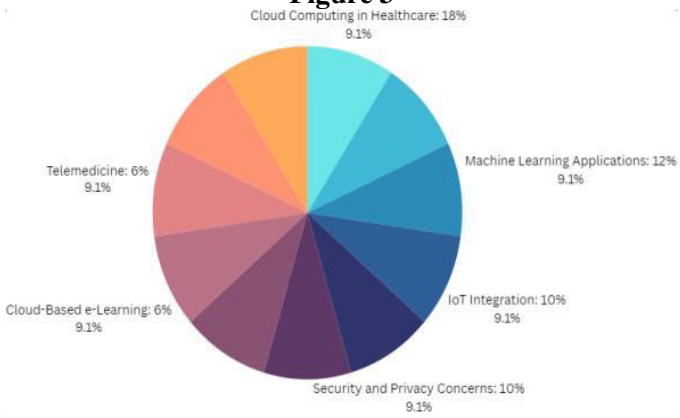
Similarly, the merging of the Internet of Things (IoT) and the use of cloud computing in healthcare. has been investigated for its potential for change in tracking patients and management of resources, emphasizing privacy and scalability difficulties while giving insights into future advances and challenges.

Healthcare cloud computing security issues have been completely researched, discovering weaknesses and possible dangers and providing crucial insights into building effective solutions to secure information about patients within cloud-based systems. Furthermore, the emphasis has been placed on secure authentication techniques supported by cloud healthcare providers to preserve patient information and increase safety precautions kept in cloud healthcare management. the factors that are driving cloud computing uptake in healthcare institutions were investigated using quantitative approaches, yielding relevant insights for ICT managers who are defining cloud-based computing policies in the medical business.

Innovative approaches for improving data security in cloud settings have been created, highlighting the method's promise in complex data processing, sickness diagnosis, imaging, medication development, and medical records administration.

Furthermore, the proposed solutions seek to provide forecasts and insights to overcome organizational hurdles during the big data adoption process in healthcare, emphasizing the potential for universal data acceptance, and implementation

Figure 3



this paper explores the transformative potential of extensive data in revolutionizing healthcare, improving patient treatment, elevating outcomes, and reducing expenses. This highlights the significance of regulations and the integration of statistical technology in scientific studies, underscoring both the challenges and opportunities linked with utilizing vast data volumes in medical contexts. These encompass concerns like information protection, security, data accuracy, and connectivity. Additionally, the study delves into potential uses of large-scale data analytics within the healthcare sector. [21] digs into the most recent research results on cloud safety and data protection, offering a complete security and confidentiality structure for identifying potential risks. The researcher analyses the effect of data breaches and illegal access on cloud computing utilization, highlighting the importance of enhanced security measures. Recognizing and overcoming these obstacles is critical for preserving the security of confidential data and retaining customer confidence as computing increases in popularity [22].

By evaluating the challenges and opportunities related to the use of enormous volumes of data for medical reasons, such as data security and confidentiality. This review additionally examined how analytical techniques for big data may be applied in healthcare, such as targeted therapy, sickness predictions, and population health management. Big data analytics may improve decision- making, patient outcomes, and cost reductions in the healthcare business, which generates a significant volume of complex data from many sources. The incorporation of massive amounts of data into healthcare is seen as vital, and it has already shown effects in areas such as personalized therapy, resource efficiency, and quick outcomes. [23].

The research paper introduces BAMHealthCloud, a cloud-based system for safe electronic healthcare storage and access to information utilizing biometric identification. The system's operational characteristics, such as speedup, mistake percentage, sensitivity, and accuracy, show that it is capable of safely handling healthcare data in the cloud. The study underlines the need for safe data access and recovery for essential medical information security, as well as the applicability of a biometric-based identification system for addressing security difficulties. The proposed paradigm is provided as a response to the security issues that have been raised about cloud-based healthcare systems. [24].

ISSN 2394 - 7780

The researcher investigates the pros and downsides of using cloud-based computing for large-scale data processing. Apart from addressing concerns regarding data security, regulations, and transfer expenses, the paper underscores the advantages of adaptability, cost- efficiency, and ease of adoption. While experts suggest that the benefits outweigh the drawbacks of utilizing cloud-based analytics for vast datasets, they emphasize the importance for businesses to thoroughly evaluate their choices before embracing cloud-based solutions. [25].

The researchers thoroughly investigate the safety and confidentiality problems that arise from the deployment of cloud-based computing in the medical sector. Following an in-depth analysis of existing research, the authors identify various security concerns, encompassing issues related to privacy, availability, confidentiality, and integrity. The article stresses the importance of adopting a comprehensive approach that effectively balances these conflicting requirements. It concludes that apprehensions about security, confidentiality, efficiency, and adaptability prevent extensive use of cloud computing in the medical sector area. The study highlights the security implications associated with cloud computing in eHealth and underscores the need for further research in this domain. [26].

Leveraging cutting-edge cloud-based technologies, the researchers explore challenges and solutions regarding security and confidentiality in e-health applications.

They identify numerous significant hurdles to address, encompassing the safeguarding of privacy, confidentiality, data integrity, and accessibility.

Additionally, they propose a fresh framework aimed at enhancing security and privacy preservation withine-health solutions. Moreover, the article delves into potential security strategies applicable to safeguarding patient information in cloud-based healthcare systems, including authentication, authorization, and multi-cloud security measures. [27].

The study paper thoroughly examines security and confidentiality problems with the vast volume of information collected in the healthcare sector. It talks about the possible advantages and difficulties of using big data analysis in population health management, illness prediction, and customized therapy, among other areas of healthcare. It also emphasizes how critical it is to put in place a thorough plan that successfully strikes a balance between security, secrecy, and efficiency. [21]

The article addresses, in summary:

1. A detailed discussion of the privacy and security problems around massive amounts of data in medical care.
2. A review of the potential benefits and challenges of analytics for large amounts of data in the field of healthcare.
3. A focus on the need to implement a methodical approach that strikes a balance between secrecy, security, and speed. [21]

ISSN 2394 - 7780

Table 2

Paper Title	Summary
eHealth Cloud Security Challenges: A Survey	The paper discusses the security, privacy, efficiency, and scalability concerns hindering the wide adoption of cloud technology in healthcare.
BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in Cloud	The paper proposes BAMHealthCloud, a cloud-based system for managing healthcare data, ensuring security through biometric authentication. The system's operational characteristics show that it is capable of safely handling healthcare data in the cloud.
A Review of the Role and Challenges of Big Data in Healthcare Informatics and Analytics	The paper explores the transformative potential of extensive data in revolutionizing healthcare, improving patient treatment, elevating outcomes, and reducing expenses. It highlights the significance of regulations and the integration of statistical technology in scientific studies, underscoring both the challenges and opportunities linked with utilizing vast data volumes in medical contexts.
Security challenges and solutions using healthcare cloud computing	The paper delves into the security and privacy challenges arising from the implementation of cloud computing within the healthcare industry. The authors identify various security concerns, encompassing issues related to privacy, availability, confidentiality, and integrity.
BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud	The paper introduces BAMHealthCloud, a cloud-based system for safe electronic healthcare storage and access to information utilizing biometric identification. The system's operational characteristics show that it is capable of safely handling healthcare data in the cloud.
Advantages and Disadvantages of Cloud-Based Computing for Big Data Analytics	The paper explores the advantages and disadvantages of employing cloud-based computing for extensive data analysis. It underscores the advantages of adaptability, cost-efficiency, and ease of adoption.
Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing	The paper explores the challenges and solutions related to security and privacy in e-health solutions using cloud computing technology. The authors propose a new framework for security and privacy-preserving in e-health solutions.

6. CHALLENGES:

The researchers investigated the usage of cloud computing in medical facilities, as well as the numerous concerns about privacy and security that develop as a result. The study emphasizes the centralized management of personal information on the cloud, which creates several security and privacy risks for people. The authors recognized various security problems, including attack susceptibility, integrity, accessibility, security, and privacy. This research also covers the present state of the science to comprehend several cloud computing strategies utilized in healthcare organizations, as well as the security problems preventing doctors and hospitals from widely adopting cloud computing [32]. The researchers noted many safety concerns with cloud healthcare systems, such as privacy, accessibility, integrity, trustworthiness, and security for multi-cloud computing. Additionally, the study offers fresh approaches to the security problems associated with cloud computing implementation in the healthcare industry [33]. The article highlights the need for security and secrecy for healthcare IoT, which is a crucial component using the usage of cloud-based computing in the healthcare sector. The researchers identified several confidentiality and security problems, including data protection, dependability, availability, and privacy. Furthermore, the paper proposes novel solutions to the concerns regarding safety and confidential data in healthcare [34]. It is important to show security and privacy concerns of data, infrastructure issues and their limitations, adoption challenges and network reliability

[35] [36]. There are also challenges in the transformative role of cloud technology enabling remote access to medical data and resources and there is a need for security and privacy measures with existing systems and the development of advanced systems to deal with these potential problems [37].

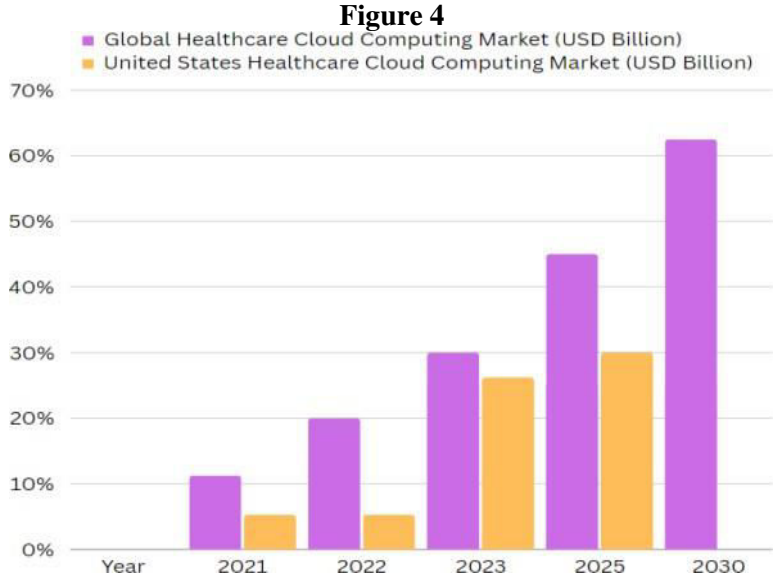
ISSN 2394 - 7780

7. FUTURE TRENDS:

With a compounded annual growth rate (CAGR) of 21.4% from 2022 to 2030, the worldwide healthcare cloud computing market, valued at USD 11.27 billion in 2021, is expected to be worth USD 62.47 billion by 2030[28]. The medical device and cloud computing sector in the United States is anticipated to expand at a compound annual growth rate (CAGR) of 22.1 per cent between 2022 and 2030, rising from USD 5.29 billion in 2022 to USD 26.2 billion by 2032[29]. According to HIMSS's Analytics Survey, more than 83 per cent of healthcare organizations already use cloud-based services. Many healthcare organizations want to use cutting-edge technology to advance these cloud computing solutions even further [29].

According to Data Bridge Industry Study analysis, the healthcare information technology cloud computing industry, which was estimated at USD 35.61 billion of dollars in the year 2022, is expected to continue to expand at an average yearly rate of 17.2% to reach USD 127.04 billion of dollars by the year 2030. [30]

Figure 4



CONCLUSION

Integrating cloud computing has changed the accessibility of data, enhancing patients' health and providing advanced innovations in the healthcare sector. And also offers multiple advantages, challenges and opportunities such as privacy of data, security, and helping in the advancement. Cloud computing has addressed many challenges and issues but leveraging cloud computing techniques can lead to more advanced patient outcomes as well as in telemedicine, streamlined operations and using bio authentication to safeguard privacy and security concerns and it has exponential growth in the coming future.

ACKNOWLEDGEMENT

I am grateful to my teacher for providing me with the opportunity to work on the "Transformative Impact of Cloud Computing on Human Health Care" project. This paper allowed me to conduct extensive research and learn new skills.

REFERENCES

[1] Lo'ai, A. T., Bakhader, W., Mehmood, R., & Song, H. (2016, December). Cloudlet-based mobile cloud computing for healthcare applications. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[2] Branco Jr, T., De Sá-Soares, F., & Rivero, A. L. (2017). Key issues for the successful adoption of cloud computing. Procedia Computer Science, 121,115-122. [3]Devadass, L., Sekaran, S. S., & Thinakaran, R.(2017). Cloud computing in healthcare.International Journal of Students' Research in Technology & Management, 5(1), 25-31.

[4] Ali, O., Shrestha, A., Soar, J. and Wamba,S.F., 2018. Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, pp.146-158.

5]Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering, 72, 1-13. [6]Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., &

Muhammad, K. (2019). The impact of the hybrid platform of the Internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151-4166.

[7] . Dang, L.M., Piran, M., Han, D., Min, K. and Moon, H., 2019. A survey on the Internet of things and cloud computing for healthcare. Electronics, 8(7), p.768.

[8] Alam, T. (2021). Cloud Computing and its Role in Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1, 108-

115.....

[9]. Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: systematic. Glob. J. Health Sci, 9(3).

[10] Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing-based health care systems. Journal of medical systems, 41(4), 50.

[11] Srivastava, P., & Khan, R. (2018). A review paper on cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, 8(6), 17-20.

[12] El Mhouti, A., Erradi, M., & Nasseh, A. (2018). Using cloud computing services in e-learning process: Benefits and challenges. Education and Information Technologies, 23(2), 893-909.

[13] Sadoughi, F., &Chenthara, S., Ahmed, K., Wang,

H. and Whittaker, F., 2019. Security and privacy- preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, pp.74361- 7438.....

[14] Jin, Z., & Chen, Y. (2015). Telemedicine in the cloud era: Prospects and challenges. IEEE Pervasive Computing, 14(1), 54-61.

[15] Zulifqar, I., Anayat, S., & Kharal, I. (2021). A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering & Electronic Business, 13(3).

[16] Lv, Z., & Qiao, L. (2020). Analysis of healthcare big data. Future Generation Computer Systems, 109, 103-110.

[17] O. Harfoushi, A. H. Akhorshaideh, N. Aqqad,

M. Al Janini, and R. Obiedat, "Factors affecting the intention of adopting cloud computing in Jordanian hospitals," Communications and Network, vol. 8, p. 88, 2016.

[18]M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," Procedia Computer Science, vol. 127, pp. 388-397, 2018.

[19]Chen, P. T., Lin, C. L., & Wu, W. N. (2020). Big

data management in healthcare: Adoption challenges and implications. International Journal of Information Management, 53, 102078. [20]Shakil, K. A., Zareen, F. J., Alam, M., & Jabin,

S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University-Computer and Information Sciences, 32(1), 57-64.

[21] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73-80.

[22] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges.

Journal of Network and Computer Applications, 160, 102642.

[23] Kraemer, F. A., Braten, A. E., Tamkittikhun, N., & Palma, D. (2017). Fog computing in healthcare–a review and discussion. IEEE Access, 5, 9206-9222.

[24]. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41, 1-9.

[25]Balachandran, B. M., & Prasad, S. (2017). Challenges and benefits of deploying big data analytics in the cloud for business intelligence. Procedia Computer Science, 112, 1112-1122.

ISSN 2394 - 7780

[26] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

[27]. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy- preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382.Journal of Medical Systems, 41(4), 50. [28]https://www.marketresearchfuture.com/reports/ healthcare-cloud-computing-market-6519

[29] https://market.us/report/healthcare-cloud- computing-market/ [30]https://www.databridgemarketresearch.com/rep orts/global-healthcare-cloud-computing-market

[31] Mekawie, N., & Yehia, K. (2021). Challenges of deploying cloud computing in eHealth. Procedia Computer Science, 181, 1049-1057.

[32] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[33] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[34] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., &

Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018, 1-9.

[35] Singh, M., Gupta, P. K., & Srivastava, V. M. (2017, November). Key challenges in implementing cloud computing in Indian healthcare industry. In 2017 pattern recognition association of South Africa and robotics and mechatronics (PRASA-RobMech) (pp. 162-167). IEEE.

[36] Khan, M. A. (2021). Challenges facing the application of IoT in medicine and healthcare. International Journal of Computations, Information and Manufacturing (IJCIM), 1(1).

[37] Gleißner, M., Dotzler, J., Hartig, J., Aßmuth, A., Bulitta, C., & Hamm, S. (2021). IT security of cloud services and IoT devices in healthcare. CLOUD COMPUTING 2021, 10.

[38] Marcu, R., Popescu, D., & Danila, I. (2015). Healthcare integration based on cloud computing. UPB Sci. Bull, 77(2), 31-42.

[39] Altowaijri, S. M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies, 249-266.

[40] Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access, 6, 19140- 19150.