JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Intelligent Healthcare with Cloud-Based Security Systems Using Temporal Anomaly Models: A Comprehensive Literature Survey

[1]Anudeep Gowda KM, [2]Devaraj V, [3]Srujan K, [4]Nitesh S, [5]Padmavathi S

[1 2 3 4]Student, [5]Assistant Professor,

[1 2 3 4 5]Computer Science and Engineering (Cyber Security),

[1 2 3 4 5]Dayananda Sagar College of Engineering, Bangalore, India

Abstract : The health industry is redefining the healthcare sector with the intersection of cloud-based security and artificial intelligence (AI).This integration is driving patient care towards a responsive. This system proposed towards a proactive, ever-observed paradigm. This pol provides a methodical examination of the technologies and techniques behind smart healthcare sys- tems that utilize the temporal aberration identification towards improved safety and foresight active performance. We schematize the research terrain, pointing out the dominant technological innovations and the dominant application challenges and re- search opportunities. Our synthesis shows that the temporal anomaly detectors which is (AI-based ones, especially LSTM) effectively solves the problem. Autoencoders have an impressive level of accuracy of as high as 98 percent on benchmarks of abnormalities in ECG detection under controlled conditions. However, the transfer of those gains to the real-life is not so smooth for deployment process, in which the latest methods are used, like federated learning remain partially adopted. By means of arranging existing work into a logical taxonomy, determining the level of technology preparedness and describing the roadmap to the development process, this survey highlights the need to make the transition between high-performance academic models and their are secure and scalable to implementation in the clinical practice.

IndexTerms **- Artificial Intelligence, Cloud computing and security, Healthcare IOT systems, Temporal Anomaly Detection models, Machine Learning, Electronic Health Records and Fed- erated Learning.**

I. INTRODUCTION

The healthcare at the modern times is changing at a rapid rate which is driven by the integrated by uninterrupted power with artificial intelligence(AI) and cloud security systems. Therefore, the integration is causing an all out trans like never before formation of patient care[1,10]. Moreover, the old reactive model of care that merely waits to attend to the situation like disaster, once it has hit, the this is no longer up to the mark of diagnosing and treating modern chronic illnesses and is becoming a challenge. which to be expensive to the contemporary healthcare systems[2]. Hence, its an urgent and critical need to eventually shift into proactive, anticipatory mechanisms which will instantly detect the slightest, last changes in the health condition of the patient prior to disaster strikes[3]. This is made possible by the technical break through called veneration of the time-related anomaly detection models[4]. These systems altogether eliminate the restrictions of the conventional, rigid and rule-based thresholds that are not only rigid, but also too many false alerts. They examine of physiological data in longer durations[4][5]. Anyways, Their actual strength is their personal, individual power reference point of each patient, so that they can point to it accurately and significantly, although non-major alterations which are consistent indicators of an oncoming health risk[5]. This foreboding ability is strong, since it creates an early diagnosis opportunity that can be extremely enhance patient outcomes in addition to providing significant reductions in the total health- care expenditure[10]. The entire intelligent healthcare model is based on a strong infrastructure. Cloud-based infrastructure platforms that are AWS(Amazon Web Services), Microsoft Azure and Google Cloud Service, this offers the enormous computing scale and storage which is necessary to cope the daily onslaught IoT, wearable devices and volume of data produced by these devices[6][7]. Therefore, Anyway working with sensitive patients health data is an indication that we need to value security and the data protection is an indivisible condition[8,9].As such any intelligent system deployed should be forged on underlying strong, none-confidence security models which do not only ensure rigid patient and privacy and regulatory compliance(e.g, HIPAA)[24,27], but also make sure that it is possible to access data in real-time and authorized, to make fast clinical decisions[9,34]. IoT-based systems, especially are still full of holes, such as Denial of Service (DoS) and other snooping technology and techniques, so the great necessity of multilayered security[6]. The smart healthcare intelligence landscape is wide and encompasses several overlapping areas such as health informatics, regulatory, machine learning and cybersecurity compliance[10,11]. This is a problem of complexity to researchers and practioners who are struggling to be confident plot potential

areas of future research. This survey directly addresses that with an all-inclusive intelligent healthcare systems analysis that incorporates cloud based security with time anomaly detection in addition[34]. Thus, Our work is surrounded by an organized literature review methodology with the help of the existing guidelines, such as pirsam to achieve replicability[12,13]. By analyzing a eventual identification of 34 good studies published since that Our survey will provide four important contributions in 2019 and 2025:(1)to provide a systematic taxonomy of the existing research territories of intelligent and safe healthcare;(2) providing an unambiguous and critical evaluation of technological abilities such as the precision of monitored and unmonitored temporal this against real- world [31] and methods of anomaly limitations;(3) identifying crucial research gaps which are especially with regards to the practical scalability of methods such as federated Learning and the ongoing interoperability issues that restrict extensive clinical use and (4) assessment of the technology Readiness Levels (TRL) required in terms of guaranteed with the real-life practical and secure implementation in real-life and complex clinical settings.

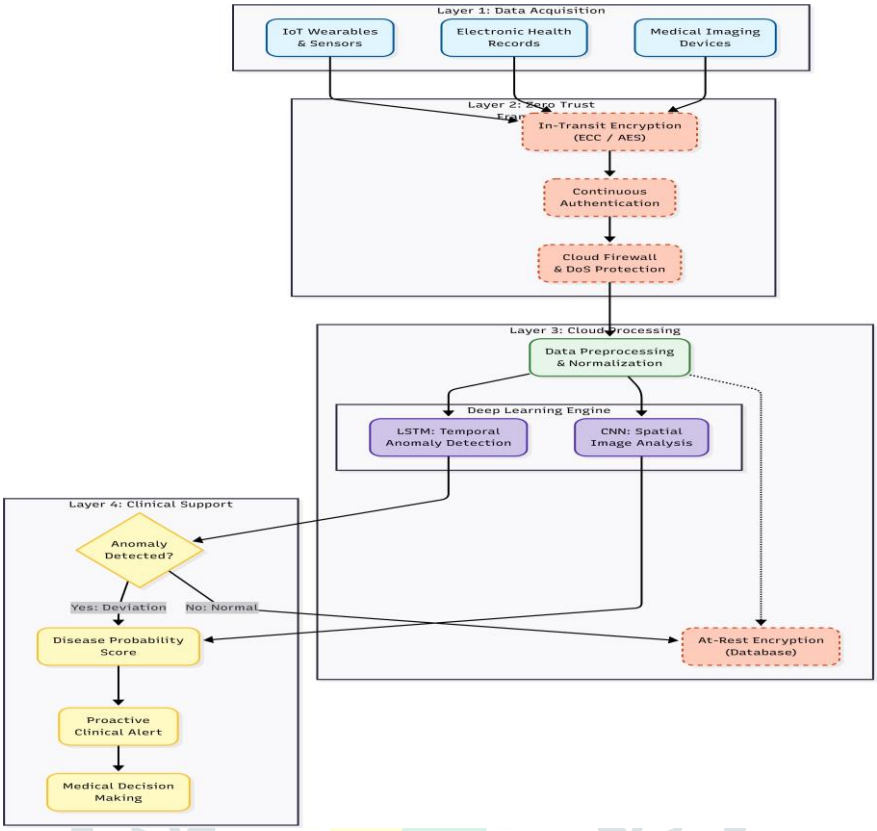

Fig. 1 system architecture.

II. LITERATURE REVIEW METHODOLOGY

A systematic literature survey was carried out with the help of a organized and strict methodology to make the findings comprehensive, objective in accordance with the accepted guidelines. To conduct systematic reviews in the healthcare informatics research. The methodology was logically done with seven major contents. the phases are: identification of the problem and literature search strategy, preferred selection criteria in the study of an elaborated data extraction procedure of critical quality assessment synthesis and analytics. Finally, the identification of gaps in research work.

A. Search Strategy used

The literature search was performed through the various academic databases such as PubMed IEEE Xplore ACM Dig- ital Library Scopus and Web of Science. The search strategy used Boolean operators to group important words (Artificial intelligence machine learning and deep learning) (healthcare medical clinical data cloud computing and cloud security) temporal anomaly time series/detection and analysis.

B. Inclusion and Exclusion Criteria

Inclusion criteria: (1)Peer-reviewed articles that were pub- lished in between 2019-2025 (2)English language publications (3)Research on AI applications in healthcare that use clouds computing components (4)Research dealing with security or aspects of privacy in healthcare systems (5)Articles discussing disease detection or time series analysis in medicine.

Exclusion criteria: (1)Non-peer reviewed articles (2)Research that lacked healthcare implementation (3) Pure theory papers having no practical implications (4) Duplicate publications (5)Studies that are not detailed enough.

C. Study Selection Process

The first search gave 847 potential articles to be studied following with the title and abstract screening 40 papers were chosen for full-text review. Quality evaluation aspects such as journals impact citation methodological regions and clinical relevance. In the last selection process 34 high-quality research papers were chosen that meet up the objectives of the research.

III. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

A. Deep Learning Architectures

The recent developments in deep learning have relegated the process of landscape of medical information analysis and different architectures that are continuously performing outstanding and transformational interoperability in various medical uses[14][15]. This is not an incremental evolution it is a significant evolution shift. In particular Convolutional Neural Networks. Conventional neural networks(CNNs) managed to make a mark as the leading technology Medical image analysis achieving accuracy in special situations which are directly comparable to and frequently competitive versus skilled clinical radiologists [16]. Additionally in dealing with the complexity that exists of time series of medical data e.g. physiological time series Recurrent Neural Networks(RNNs) and their potential form. The Long Short-Term Memory(LSTM)network and is the one that is proven remarkably effective and another interesting example is the behaviour of LSTM autoencoders that have been reliably recorded a high level of 98 percent accuracy in electrocardiogram anomaly detection[17]. There- fore, these findings all add up emphasize the dramatic power of deep learning to improve the accuracy and effectiveness in the clinical practice.

B. Traditional Machine Learning Applications

Further Although deep learning reigns in some fields like Conventional Machine Learning(TML)algorithms are still there significant to healthcare analytics specially where data sparsity or the requirement of explicit model interpretability is paramount[19][20]. These algorithms are not novel but on the contrary they offer strong solutions that are proven for instance Random Forest algorithms always provide strong and reliable conformance in challenging clinical decision support systems as confirmed by their ability to record an impressive 98.34 percent accuracy of complicated risk forecasting models[21]. Moreover at the same time the Support Vector machines (SVMs) keep on proving their efficacy in key patient classification tasks. Therefore in ensemble has been used like it is a smart combination of the results of the several methods and also algorithms this improves system reliability and enhances the system comprehensive the performance envelope[22]. Consequently TML thus is a working force and interpretable spot in the contemporary analytics toolkit.

C. Natural Language Processing Applications

Natural Language Processing (NLP) The area of Natu- ral language processing(NLP)is a critical one and extremely valuable power in healthcare which the core focuses onhewhat was fundamental to the clinical documentation process automation and the effective extraction of information on bulky and unstructured medical records[25][26].Furthermore the implementation of superior NLP algorithms provides demonstration and immediate clinical worthiness. More im- portantly such systems have proven that to get a 40 percent cut in requirements of the documentation time.

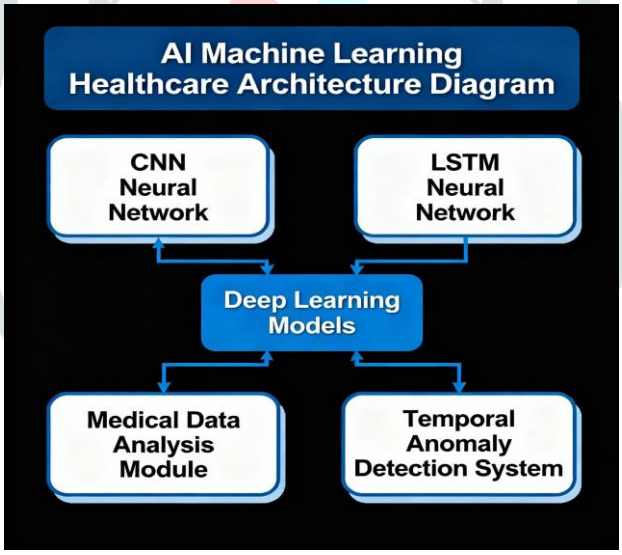

Fig. 2. AI and Machine Learning in Healthcare.

IV. CLOUD COMPUTING AND SECURITY FRAMEWORKS

Cloud computing has now become the backbone to mod- ern healthcare delivery like main cloud provider such as Amazon Web and services (AWS) Google cloud platform(gcp) Microsoft Azure being the main ones which are delivering holistic healthcare [30][31]. Multi cloud architectures do shows67 percent user enhancements and Distributing workloads through several individuals can be used to achieve additional and efficiency in improving the performance through cloud vendors and minimizing vendors dependency [32].

Framework	Description	Advantages/Challenges
Zero Trust	This security model is based on the strict concept of trusting no one and authenticating everything and the model requires constant authentication and stringent access control of all users and devices irrespective of their location [27].	Introduces to adaptive access controls and not easy to apply.
AES	It is a framework that is needed to offer powerful of data security that is not only computationally powerful but also meets the demands of high volume of real time data processing in the clinical settings [34]..	Computationally efficient vulnerable to implementation means failures
ECC	The cryptographic technique provides a good security guarantee and also has the advantage of using the reduced key sizes which ensure high efficiency and is a very suitable option when IoT components have resource limitations in a healthcare setting [26].	IoT friendly and more complicated to use than RSA.

TABLE I. CLOUD COMPUTING AND SECURITY FRAMEWORKS

V. INTERNET OF THINGS AND WEARABLE DEVICES IN THINGS.

With the emergence of the Internet of Things (IoT) the concept of patient care shifting it towards the all-pervasive surveillance which means the continuous monitoring. This is the integration that involves the use of high-end wear- ables and medical-grade sensors that enables the real time tracking of physiological vitality of the parameter such as hemodynamic parameters to blood oxygen saturation in real time[7][8].This is high quality and incessant of data stream is required to drive the temporal anomaly detection models we discuss that it gives them the ability to have personalized subtle for the critical deviations[7][8].However this immense jump in connection preconditions an equally decisive that are security vulnerability. IoT systems in healthcare have been made vulnerable to numerous attacks that are such as crippling Denial of Service (DoS)attacks snooping and direct sensor intrusions[6]. The interests are too high research proves that a lot of them companies that employ such systems are attacked by cyberattacks badly indicating the intolerable requirement of strong security frameworks [9]. This risk is a multilayered one which needs to be mitigated. This implies forced device level encryption using authenticated communications and high level network segmentation to separate vulnerable machines and the continuous software upgrades[6][9].These preventive measures are essential to save the sensitive data of a patient that moves through the network edge to the cloud[7,8].

VI. TEMPORAL ANOMALY DETECTION

Method	Description
Supervised Learning	Such a method requires the employment consistently train on labeled data and never the less performs well in terms of accuracy especially when high quality adequate training of instances are made available [31][19].
Unsupervised Learning	This is a very successful methodology where data of labeling takes the form of scarcity or absence of applying such methods as isolation forests and all sorts of autoencoders to notice deviations from normal pattern [31].
Real-time Processing	his approach is critical to working deployment as it demands a close balancing precision in computational efficiency to logically guarantee provision of timely alerts to healthcare providers [4][5].

TABLE II. TEMPORAL ANOMALY DETECTION METHODS

VII. CLINICAL DECISION SUPPORT SYSTEMS

Artificial Intelligence based Clinical Decision Making Support Systems (CDMSS) are not only a luxury but that needed a jump in the modern healthcare delivery so they move past simple data imaging to render actual forecasting clinical sup- port[32].Said that the systems serve as the center of operation layer of intelligent that is combining the strong machine learn- ing algorithms of healthcare Deep learning models and Natural Language Processing(NLP).To improve the accuracy of diag- nosis and the complex treatment recommendations[10].Vast application of the advanced CDSS and the in particular those based on state of the art temporal anomaly detection is not the technical refinement but this is a direct intervention on improved quality of care. The clinical impact is clear patient outcomes have been found to be improved and the quantifiable decreases in complications on a range of chronic conditions [32][10]. Capability of CDSS to process instantaneously large amounts of customized patient information and clinical with knowledge of one can make fine tailor made interventions. This proves them to be of paramount importance to the future of proactive healthcare systems [10].

VIII. IMPLEMENTATION CHALLENGES AND LIMITATIONS

Although the accuracy of the AI models is convincing when it comes to controlled environment such that there are many limitations to trolled in the lab environments some of which are important that indirectly prevent the effective implemen- tation of smart healthcare and real world clinical systems. The main one critical gap is that developed privacy sensitive machine learning similar to federated learning(FL) between academic notions and scalable operations[33]. The practical and successful application of the federated learning is still restricted. This reflects a crucial abacus between theoretical possibility and practical reality[33]. Three barriers that are the cause of this bottleneck in the deployment implicit technical complexity of running distributed models in diverse hospital structures regulatory ambiguity concerning to the cross juris- dictional data sharing and the comprehensible resistance of the new technologies in the institution[34]. The basic issue of the interoperability is that the capability of that to share and use information in different healthcare IT systems that must be used in as well remains as a major obstacle[34].In the absence of efficient system integration of the promise of smooth and smart tracking of patients remains fractured. This brings out the necessity to have standardized security and information exchange systems to unleash the potential of these high technologies in healthcare systems.

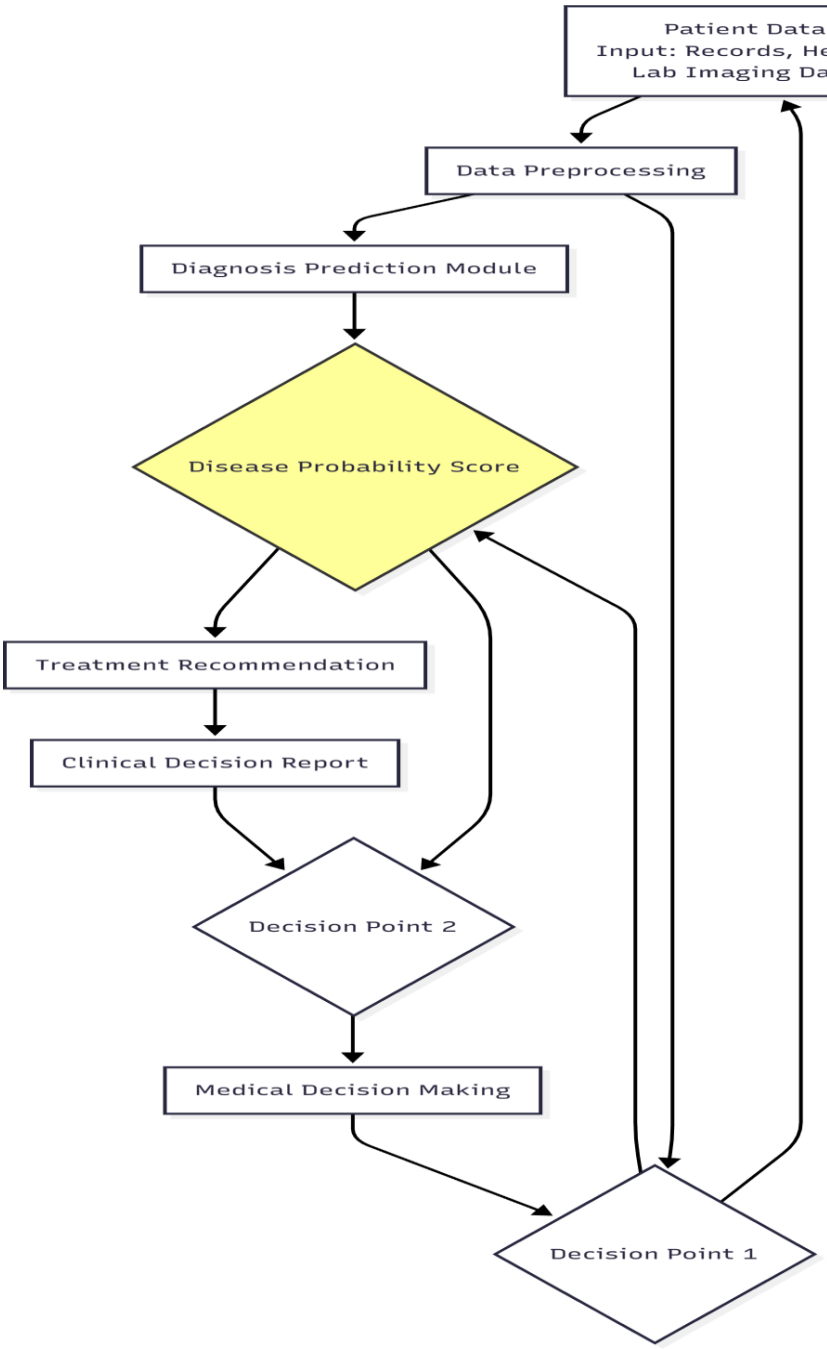

Fig. 3. Clinical Decision Support Systems.

CONCLUSION

To sum up this methodological literature review demonstrates a intelligent healthcare systems landscape that is rapidly emerging and becoming promising. The pressing that is the necessity to combine that this the characteristic of it in the data centers that are based in the clouds and have sophisticated time related to security systems that are the capabilities of anomaly detection[1,34]. Through analysis of 34 research articles of high quality that were published in the last two years(since 2019). We have demonstrated great technological maturity in 2025. The core AI applications[10]. Namely that are sophisticated systems LSTM autoencoders which are deep learning models that are known to accomplish superior quality in the detection of the anomalies in time series. This solidly determines the technicality of proactive patient monitoring[17][31]. There are also cloud based architectures which are offering the necessary scalability and computing capability required to handle massive amounts of IoT data. This is supported by the process of improve strong security systems such as Zero Trust and ECC compliance and data protection[27][26]. However our survey points out an obvious difference between this high technical potential and the fact of working deployment[34]. Our key findings lead to significant lapses. These consist of the real of the limited advanced privacy preserving and rate of world implementation such methods as federated learning[33] and mass cable Challenges of system interoperability in different hospitals settings[34]. Regardless of the reason that it was time to bring intelligent healthcare to a close theoretical achievement to a general clinical fact in future the studies need to be aimed at combating such hurdles. It must focus on building scalable common security systems and combined information sharing protocols so these are necessary to fill the remaining gap between theoretical behavior and real clinical implementation[9][34].

REFERENCES

[1] S. K. Marimekala, J. Lamb, and R. Epstein, "Using AI and Big Data in the HealthCare Sector to help build a Smarter and more Intelligent HealthCare System," in *IEEE World AI IoT Congress (AIIoT)*, 2024.

[2] V. Vasamsetty et al., "Anomaly Detection in Cloud Healthcare Net- works using Temporal Convolutional Network," *International Journal of Biomedical Engineering and Medical Research*, vol. 2, no. 88, pp. 1-12, 2019.

[3] S. Sridharan, S. Deivasigamani, and R. Rajesh, "Enhancing Healthcare through AI Deep Learning: A Human-Centric IoT Advisory System Cloud," in *2nd International Conference on Sustainable Computing and Smart Systems*, 2024.

[4] M. Nawaz et al., "Cloud-based healthcare framework for real-time anomaly detection," *PMC*, vol. 9, pp. 1-15, Dec. 2022.

[5] S. A. Samriya et al., "Enhancing Healthcare Data Privacy in Cloud IoT Networks with Real-Time Anomaly Detection," *Elsevier Science Direct*, 2025.

[6] S. Nasiri et al., "Security Requirements of Internet of Things-Based Healthcare System," *PMC*, vol. 7, pp. 1-18, Apr. 2019.

[7] S. Abdulmalek et al., "IoT-Based Healthcare-Monitoring System towards Improving Patient Outcomes," *PMC*, vol. 9, pp. 1-12, Oct. 2022.

[8] M. S. Shaw and A. Gohel, "Role of artificial intelligence in health monitoring using IoT based wearable sensors," *Elsevier Science Direct*, 2025.

[9] A. Deshmukh et al., "A Review on IOT Security Challenges in Health- care," *DPCO Engineering Pune*, 2021.

[10] J. Bajwa et al., "Artificial intelligence in healthcare: transforming the practice," *Future Healthcare Journal*, vol. 8, no. 2, pp. e188-e194, 2021.

[11] A. Habehh and S. Hussain, "Machine Learning in Healthcare," *Current Genomics*, vol. 22, no. 4, pp. 291-300, 2021.

[12] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *PLoS medicine*, vol. 6, no. 7, p. e1000097, 2009.

[13] K. Stansfield, S. J. Walsh, and L. A. Morgan, "Systematic literature reviews in health informatics: A review of current methods," *Journal of Biomedical Informatics*, vol. 46, no. 5, pp. 930-939, 2013.

[14] G. Litjens et al., "A survey on deep learning in medical image analysis," *Medical Image Analysis*, vol. 42, pp. 60-88, 2017.

[15] I. S. Ismaili, A. Idrissi, and D. Ghoujdami, "Deep Learning for Anomaly Detection in Healthcare: A Systematic Review," in *IEEE/ACS 16th Inter- national Conference on Computer Systems and Applications (AICCSA)*, 2019, pp. 1-8.

[16] A. Esteva et al., "A guide to deep learning in healthcare," *Nature Medicine*, vol. 25, no. 1, pp. 24-29, 2019.

[17] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long Short Term Memory Networks for Anomaly Detection in Time-Series Data," in *Proceedings of the European Symposium on Artificial Neural Networks*, 2015.

[18] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5-32, 2001.

[19] S. R. Ahmad, A. K. Singh, and M. Hanmandlu, "A review of machine learning techniques in healthcare," in *International Conference on Signal Processing and Communication (ICSC)*, 2018, pp. 132-137.

[20] R. K. V. S. Raj, K. S. Kumar, and M. P. Kumar, "A robust random forest based clinical decision support system for predicting heart disease," in *IEEE International Conference on Smart Technologies and Manage- ment for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2017, pp. 210-215.

[21] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273-297, 1995.

[22] Y. Wang, L. Wang, M. Rastegar-Mojarad, et al., "Clinical information extraction applications: a literature review," *Journal of biomedical in- formatics*, vol. 77, pp. 34-49, 2018.

[23] S. Devlin, J. Chang, M. W. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics*, 2019, pp. 4171-4186.

[24] Amazon Web Services, "HIPAA Compliance," AWS Whitepaper, 2024.

[25] S. K. Sood and S. Singh, "Multi-cloud architecture for healthcare services," *Journal of Medical Systems*, vol. 42, no. 9, p. 165, 2018.

[26] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.

[27] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, 2010.

[28] M. A. F. Al-Husainy, "A survey of edge and cloud computing for IoT healthcare applications," *Journal of Network and Computer Applica- tions*, vol. 177, p. 102945, 2021.

[29] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34-42, 2017.

[30] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found a lurking threat in IoT-based healthcare systems," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 111-122.

[31] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, pp. 1-58, 2009.

[32] R. A. Greenes, *Clinical decision support: the road to broad adoption*, Academic Press, 2014.

[33] K. Bonawitz et al., "Towards federated learning at scale: System design," in *Proceedings of the 2nd SysML Conference*, 2019.

[34] J. J. P. C. Rodrigues et al., "Analysis of the Security and Privacy Requirements for Cloud-Based Electronic Health Records Systems," *J Med Internet Res*, vol. 15, no. 8, p. e186, Aug. 2013.