Ingénierie des Systèmes d'Information
Vol. 30, No. 1, January, 2025, pp. 43-59
Journal homepage: http://iieta.org/journals/isi

An Enhanced Model for Smart Healthcare by Integrating Hybrid ML, LSTM, and Blockchain

Chanumolu Kiran Kumar[1], G. Muni Nagamani[2*]

[1] Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Deemed to be University, Vaddeswaram 522302, India
[2] Department of Computer Science & Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada 520008, India

Corresponding Author Email: nagamani@aliet.ac.in

https://doi.org/10.18280/isi.300105

Received: 12 August 2024
Revised: 17 November 2024
Accepted: 15 January 2025
Available online: 25 January 2025

Keywords:
healthcare, Internet of Things (IoT), Artificial Intelligence (AI), blockchain, machine learning, Long Short Term Memory (LSTM)

ABSTRACT

Conventional healthcare systems are traditionally challenged by fragmented data, lack of predictive insights, and security concerns, which spouse their effectiveness and efficiency. This paper will cover these gaps by developing an integrated Smart Healthcare System leveraging the power of the Internet of Things and Artificial Intelligence processes. To that end, we have proposed a holistic model that integrates several advanced methodologies to help in enhanced disease prediction and patient monitoring, with data security and privacy protection. We further apply the Hybrid Machine Learning (ML) models specifically; Random Forest Classifier integrated with k-means clustering for the prediction of diseases. This will cluster patients according to their similarity in health characteristics and provide an accurate disease risk prediction with an accuracy of 85-90%. Accordingly, Long Short Term Memory (LSTM) networks will be used for deeper timestamp series analyses with the following input sets: predicted disease probabilities, time-stamped health monitoring data, and patient lifestyle information sets. This model is outstanding both in regard to forecasting disease progression and in detecting anomalous health events with less than a 5% false positive rate. For protection and integrity of the data, we will use an Ethereum blockchain framework with respective smart contracts. The approach will provide secure, immutable health data storage and controlled, traceable access in full compliance with the requirements of various data protection regulations, such as GDPR. What's more, differentially private computations on encrypted data samples are guaranteed by combining homomorphic encryption methods with differential privacy techniques. The former ensures that in any kind of data analysis, at the point of execution, individual patient privacy is maintained, while the latter ensures an accurate, aggregated health data insight for different scenarios. By incorporating these methods, a robust smart healthcare system would be developed, one which, other than the ability to predict and monitor the progression of a disease very precisely, was able to protect patients' data and respect privacy. The same work has far-reaching implications in achieving better patient outcomes through earlier interventions and provision of increased security to the data, apart from enhancing trust in digital solutions for healthcare.

1. INTRODUCTION

The coming of the Internet of Things and Artificial Intelligence has disrupted many sectors, not excluding healthcare, where the cure perhaps has been very hard. Traditional healthcare systems are normally inefficient, characterized by siloes of data, and low ability to predict. These deficiencies therefore call for the development of sophisticated, integrated models that take advantage of advanced technologies in improving disease prediction, patient monitoring, and security of data and privacy protection. Recent advances in machine learning and deep learning for medical diagnosis and prognosis look very promising. Hybrid models, combinations of different algorithms, hold great potential to predict the possibilities or occurrence of a disease with reasonable accuracy. In this work, we have combined a Random Forest Classifier with k-means clustering to segment patients into clusters of persons with similar health characteristics to improve the accuracy in the prediction of disease probabilities.

Predicting disease occurrence, however, is not the whole solution. Its continuous monitoring, coupled with accurate forecasting of the progression of a disease, is equally important. Long Short-Term Memory (LSTM) networks constitute a kind of RNN specifically applied to timestamp series analysis and have shown a great deal of efficacy in predicting future health events from historical data samples. LSTMs combine probabilistic outputs of disease risk, time-

stamped health monitoring data, and patient lifestyle information to yield insight into disease progression and early anomaly detection. This information is very sensitive for a patient in this domain; thus, its handling is very important from the integrity and security point of view. Blockchain technology helps in offering decentralized, immutable ledgers to store health data samples securely and have them accessed in a controlled manner. This research has ensured that patients' data is retained securely with the Ethereum blockchain and smart contracts, while the access to the data will be transparent and traceable with strict adherence to rigid data protection regulations like General Data Protection Regulation. Moreover, this research has also established privacy through Homomorphic Encryption and Differential Privacy techniques. These methods document the various computations on encrypted data without really exposing sensitive information, ensuring that individual patient privacy is retained while the resultant, valuable, aggregated data insights can serve a host of different scenarios. This paper comes up with an integrated model combining these advanced methodologies in order to build a robust Smart Healthcare System. The proposed model in the present study enhances predictive accuracy in health monitoring systems while ensuring data security and privacy. It would be a comprehensive and integrated approach to significantly improving patient outcomes, building trust in digital healthcare solutions, and paving the way for more intelligent, efficient, and secure healthcare systems.

1.1 Motivation and contribution

The multifaceted challenges in modern healthcare systems make this research very timely. Conventional healthcare infrastructures possess fragmented data sources, lack adequate predictive analytics, and have huge security vulnerabilities-all of which badly hamper appropriate disease management and care delivery to patients, influencing health outcomes and reducing efficiency. This integration of IoT devices with Artificial Intelligence in their functions presents a great opportunity for the eventual revolutionization of healthcare delivery. Assured enhanced accuracy in disease prediction but continuous patient monitoring with robust data protection is achievable by leveraging IoT and AI to ensure a more cohesive, predictive, and secure healthcare environment. It is to address these critical needs that this research has been driven to develop an innovative model that will integrate advanced machine learning techniques, timestamp series analysis, blockchain technology, and privacy-preserving methodologies into a comprehensive smart healthcare system. The major contributions from the research are related to the development of an integrated model that substantially improves the current state of healthcare technology. In the first instance, this work presents a novel approach to disease prediction with the help of Hybrid Machine Learning Models-Random Forest Classifier with k-means clustering. The application of this model, therefore, will let patients fall under clusters having similar health characteristics and enable a more efficient prediction about the occurrence of diseases with an accuracy of 85-90%. All this granularity in prediction is very important for determining high-risk patient groups and tailoring preventive measures.

It also applies Long Short-Term Memory networks in the analysis of timestamp series data for diseases to be predicted, combining probabilities with time-stamped health monitoring data and patient lifestyle information. This will aid the system in predicting the progression of diseases accurately and detecting anomalies in health, therefore performing timely interventions for better patient outcomes. Subsequently, it is enhanced by the integration of LSTM networks that solve dynamic characteristics of health data with its continuance and adaptive monitoring, which forms a very important part in any effectual management of diseases. Another integral fact about this research relates to blockchain technology, which has been integrated into enhancing security and integrity in data storage. The model proposed will use Ethereum Blockchain and Smart Contracts, technologies that will ensure a rather safe storage of health data, and access to it can thus be controlled and traced minutely. This approach safeguards patients' information from third-party access, besides adhering to the stringent data protection regulations, for instance, the GDPR. Blockchain technology helps solve a very critical issue-and that is data tampering and unauthorized access-by providing transparent and immutable records of all transactions for data.

The research takes into consideration these privacy concerns through the application of Homomorphic Encryption and Differential Privacy. It is a special type of encryption called homomorphic encryption, which allows one to do computations on encrypted data without really knowing what it is. In this case, it is going to guarantee that no sensitive information related to specific patients will be disclosed in the process of data analyses. Differential privacy does this through the addition of noise into the insights derived from aggregated data and makes them unable to identify particular patients, yet remaining accurate and useful. This dual privacy-preserving approach in the analytics phase makes certain that high-accuracy computability in the system is coupled with valuable health insight generation, wherein Patients' confidentiality is not compromised. In a nutshell, this work substantially contributes to smart healthcare by fusing cutting-edge ML/DL techniques with secure blockchain and privacy-preserving methodologies. Besides enhancing the predictive abilities and monitoring accuracy, the proposed model ensures data security and privacy are not compromised. Facing the limitations of conventional healthcare systems, the research works toward further improving intelligent health care delivery, Making it more efficient and secure for better patient outcomes and increased trust in digital health solutions. Their inventive combination gives a big advance in the development of next-generation healthcare systems to meet all kinds of challenging demands experienced in modern healthcare surroundings.

2. REVIEW OF EXISTING MODELS FOR HEALTHCARE ANALYSIS

(1) Machine learning methods for intelligent healthcare principles and advantages

ML, particularly by way of hybrid models, deep learning, and clustering, has increasingly been used to predict the onset and progression of diseases as well as risk stratification of patients. Methods of applying the Random Forest Classifier with k-means clustering, like in this study, provide a multi-step approach where patients are first clustered by health characteristics and these clusters will increase predictive accuracy for disease probability. It allows for more precise definition of the 'at-risk' groups and helps in more directed healthcare delivery. In addition, LSTM networks are used for temporal analysis in healthcare which facilitates the

continuous monitoring of disease progression and anomaly detection. The long-term dependencies in health data can be captured by the LSTM model, which is very useful when interventions need to be provided on time, which can be based on real-time health changes. Limitations Machine learning models require massive computational resources, especially deep architectures that include LSTMs, which leads to huge amounts of memory and processing requirements. Further, as noted NLP in healthcare is a vital feature extraction and interpretation of clinical data in terms of clinical outcomes, but it requires significant computational ability. If not well supported by a robust computational infrastructure, this makes health care applications large scale or even real time challenging. Metaheuristic algorithms for routing for energy efficiency suffer with high computational complexity. Systematic Comparison Hybrid ML models like Random Forest Classifier integrated with clustering, as applied in this study, are seen with notable improvements in predicting accuracy above the traditional single-step classification methods. Comparative studies, reported lower prediction accuracy at 86.1% with an indication of the advantage of combining clustering with classification towards better specificity for identification of a high-risk group. Here, for anomaly detection, the employed LSTM model was good, as it showed a lower value of 0.038 in MAE against 0.060 reported by other methods. It can be easily seen that LSTM indeed has strong ability to learn temporal dependencies important for the domain of healthcare.

(2) Blockchain-based security methods principles and benefits

The implementation of blockchain technology, in particular with smart contracts, can establish an immutable and decentralized record of healthcare data, thus further enhancing the integrity, security, and compliance of data with regulatory frameworks, such as GDPR. Ethereum Blockchain with smart contracts, as applied in this paper, enables the secured storage of health data and controlled access to prevent unauthorized access and tampering of the data samples. This is also highly traceable, ensuring accountability for every access of the data samples. Blockchain enabled key management and blockchain for access control in IoT-based healthcare systems make evident how blockchain protects IoMT devices using strong authentication, thereby enhancing the privacy of healthcare data samples. Limitations However, blockchain implementations are usually computationally intensive, as seen in where blockchain-based EMR sharing, notwithstanding all the advantages it had, was marred by high computational overhead and latency-related issues. Moreover, blockchain systems usually tend to be expensive, and managing blockchain infrastructure may severely limit scalability. This is especially problematic in environments of high transactions such as smart health where fast and scalable solutions are a requirement. Systematic Comparison Compared to this research, the integrity on data is better provided by the Ethereum Blockchain-based model, at 100% compared to 98% and 96% as compared with other models. That kind of approach access control with smart contracts also limits all unauthorized attempts at access, thus providing more security layers. Alternative solutions, such as lightweight encryption in IoT data sharing though efficient, suffer from severe encryption overheads, implying a trade-off between efficiency and security in resource-constrained devices & deployments.

(3) Federated learning and privacy-preserving techniques

Principles and Benefits Modern health care systems rely on privacy-preserving methodologies, for example federated learning and differential privacy for secure data sharing that does not compromise the confidentiality of patients. Federated learning is understood to mean collaborative learning of models across distributions of health data without transferring raw data to a central server, and because of this, sensitive information remains localized and improves privacy, Data offered protection by the application of homomorphic encryption and differential privacy methods used in this research. In case of homomorphic encryption, data computation on encrypted data is very important to ensure that at the time of analysis, there is a guarantee of patient privacy. Differential privacy adds noise to the set of data in such a way that it minimizes the identification of patients in the data; however, the noise added does not affect the amount of required precision in any given analysis. Limitations Federated learning is computationally expensive and requires robust network infrastructures and high data transfer rates, but it preserves privacy. Homomorphic encryption is also computational-costly; hence processing time is typically delayed in real-time healthcare applications. Comparative Systematic In contrast with other works, the privacy metrics obtained in this research, specifically the minimal privacy loss ϵ=0.7 and high private result accuracy at 97%, indicate significant improvements over traditional models based solely on federated learning alone which often display greater privacy loss and reliance on network infrastructure. The two-layer mechanism of privacy used here in this context achieves a high level of privacy preservation with minimal utility loss compared to privacy frameworks that use only one technique.

(4) IoT and cloud-based integration for scalable healthcare systems

Principles and Benefits IoT devices and cloud computing are the basics of scalable, real-time smart health care. Green health care frameworks cloud-based support large-scale health monitoring. This is due to the storage and processing of large amounts of patient data in the cloud, made possible through IoT devices facilitating real-time data collection. AI-enabled edge computing represents another method through data processing near to the source location, thus fastening data processing and overall system response time. Limitations Despite the advantages of scalability in IoT-cloud frameworks, they have a tendency to be prone to network security risks since data in motion security relies on a robust cloud infrastructure. Additionally, edge devices lack in considerations about their provision of computation power and energy efficiency, thus curtailing their applications into resource-intensive ones. Green IoT frameworks also depend on device security, which is also seen to be problematic in less structured environments.

2.1 Systematic comparison

More precisely, compared with the centralized cloud models, edge computing reduces latency and improves response delays at the cost of reduced computational power, which remains limited in edge devices & deployments. The framework of cloud-IoT applied in the present work offsets the constraints, thus maintaining a balance between scalability, security, and privacy with the aid of blockchain-based checks on data integrity and robust privacy-preserving techniques. Conclusion of Systematic Comparison Systematic assessment

of the presented approaches shows that each category presents its own point of strength, while the computational requirements, reliance on strong infrastructures, and expenses go across all. The integrated model developed within this study-a hybrid of ML, LSTM networks, Ethereum Blockchain with smart contracts, and privacy-preserving encryption-builds a bridge over the existing solution weaknesses and simultaneously solves them. The proposed solution incorporates an advanced learning machine, decentralized security frameworks, and robust privacy protection. These features make it a better competitor against standalone approaches and, therefore, offer a comprehensive, scalable, and secure smart healthcare system that meets the multifaceted demands of modern healthcare environments.

2.2 Summary of review analysis

A critical review of the recent studies in this regard has brought out the diversified approaches and methodologies adopted within the domain of smart healthcare, which in one way has contributed to the overall progress but at the same time also offers a separate set of limitations and challenges. Pradhan et al. [1] discussed the role of AI together with 5G communication in showing how the synergy of these two can further enhance real-time decision-making and security in healthcare systems. This method has huge potential but is sadly limited because of its high implementation costs and strong dependence on 5G infrastructure. In the domain of healthcare, as evidenced by Zhou et al. [2], NLP played a relevant role in enhancing the interpretation of data through better feature extraction and analysis. However, the complexity and large computational resources demanded by the techniques of NLP restrict their application. Alruwaili et al. [3] shows that blockchain enabled smart Health care system using jelly fish search optimaizatipn algorithm for disease detection with high accuracy. Limitations Federated learning is computationally expensive and requires robust network infrastructures and high data transfer rates, but it preserves privacy, according to Akter et al. [4].

Saini et al. [5] proposed a lightweight smart-contract-based transaction prioritization scheme, which can optimize the handling of electronic medical records. This would increase scalability issues wherein high transaction volumes for different scenarios are to be taken into consideration. Thapliyal et al. [6] shows how blockchain provides protection with strong authentication, and how it will be suitable for healthcare domains. Raina and Jha [7] work with Hidden Markov model enhanced with probabilistic approach for better prediction.

Syu et al. [8] discussed AI-empowered edge computing, which provided improved data processing speeds and increased accuracy; however, such work is still fundamentally limited in capability and power consumption by edge devices and deployments. Wu et al. [9] applied blockchain in secure sharing of electronic medical records, ensuring privacy but with high computational overhead. Islam and Bhuiyan [10] used a cloud and IoT-based green healthcare framework, thus ensuring scalable solutions but are dependent on the security of the Cloud and the IoT devices. Mallick et al. [11], who combined blockchain with geospatial web services, improved efficiency in data management and was limited to problems like accuracy in data and scalability. Ali et al. [12] contributed a comprehensive survey about federated learning for privacy preservation, focusing more on better privacy and collaborative learning at the cost of robust sets of network infrastructures.

Wazid et al. [13] focused on ransomware attacks against a blockchain-enabled security framework that offers higher security but is encumbered with issues of complexity and cost. Li et al. [14] proposed a federated learning approach for the preservation of privacy concerning healthcare data analysis, achieving effective analysis but relying on federated infrastructure. Abdeen et al. [15] reviewed the various elements involved in smart health systems, overlooking them from a general perspective and, hence, identifying key challenges and possibilities but failing to provide solutions. Egala et al. [16] investigated intelligent blockchain applications that enhance security and privacy but emerge with integration complexities and high computational burdens. Almas et al. [17] proposed context-based adaptive fog computing that enhances the trust of time-critical systems and, as a result, has limitations on fog infrastructure capabilities. Gao et al. [18] worked on resource allocation assisted by IoTs, which ensured efficient management and thus became dependent on IoT infrastructures. Li et al. [19] designed a fog computing healthcare access control scheme that has secure management but high cost and complexity. Hajjej et al. [20] proposed efficient motion detection with deep learning that provided an accurate analysis, but high computational power and sensor accuracy are prerequisites. Bao et al. [21] have presented the IoT healthcare secure data sharing method-based lightweight encryption that gives high efficiency but suffers due to encryption overhead bounds. Lin et al. [22] have used neurocomputing for smart home energy management; it showed improvements in forecasting and management but depended on AI models and accuracy of data. Rana et al. [23] used metaheuristic algorithms to achieve energy efficiency for optimization of routing in health systems at very high computational costs. Islam et al. [24] reviewed various IoT device capabilities and protocols; this provided insights but did not mention any implementation strategy in detail. Fan et al. [25] contributed to the topics of smart city security, identifying some of the important challenges and solutions of IoT security with no specific focus on healthcare scenarios.

Table 1 discusses some of the various approaches used in the development of smart healthcare systems and describes how these, although increasing valuable input and advances, also represent notable challenges and limitations. A clear need to integrate different methodologies in order to meet such complex needs of modern healthcare environments has been underlined. This paper proposes a Smart Healthcare System that exploits the power of various advanced technologies in a Hybrid Machine Learning model, Long Short-Term Memory network, Ethereum Blockchain with Smart Contracts, and Homomorphic Encryption with Differential Privacy Techniques. This will improve the accuracy of disease prediction and progress monitoring, ensure patients' data security, and preserve their privacy.

The authors have combined a Random Forest Classifier with k-means clustering to develop a Hybrid Machine Learning model that significantly improves the accuracy in disease prediction to 90.2%. This can be considered an improvement over previous methods, for instance, the accuracy of 86.1% reported. The LSTM network, as demonstrated in this research, works nicely in predicting the progression of a disease and the detection of anomalies, with a resultant very low MAE of 0.038 against the MAE presented by other methods, which was 0.060. The integration of

Ethereum Blockchain with Smart Contracts resolves the very essential challenge of data security, hence guaranteeing data integrity at 100%, against 98% and 96%, recorded. It is a high-security framework that forms cases of data tampering and unauthorized access, hence more trust in this system. Another critical aspect that the proposed model has addressed is the preservation of privacy through techniques of Homomorphic Encryption and Differential Privacy. It ensures that the amount of loss of privacy, ϵ, remains very minimal at 0.7, while undesired utility loss is only 3.0%, thus maintaining accuracy in private results at 97.0%. This turns out to be better in preserving privacy when compared to methods that demand a more robust set of network infrastructure.

Table 1. Empirical review of existing methods

Ref.	Method Used	Findings	Results	Limitations
[1]	AI-Assisted 5G Communication	Integration of AI and 5G enhances smart healthcare capabilities	Improved real-time decision-making and security	High implementation cost and dependency on 5G infrastructure
[2]	Natural Language Processing (NLP)	NLP techniques facilitate better data interpretation in healthcare	Enhanced feature extraction and data analysis	Limited by complexity and computational requirements
[3]	Blockchain with Jellyfish Search Optimization	Blockchain enhances security; dual-pathway CNN improves diagnostics	High accuracy in medical diagnostics	High computational cost and complexity
[4]	Federated Learning-Based Privacy Protection	Federated learning ensures privacy while enabling data sharing	Improved privacy and data security	Requires complex infrastructure and high data transfer rates
[5]	Lightweight Smart-Contract-Based Transaction Prioritization	Smart contracts optimize transaction handling in healthcare	Efficient EMR handling and prioritization	Scalability issues with high transaction volumes
[6]	Blockchain-Authenticated Key Management	Blockchain-based key management improves security in IoMT	Enhanced authentication and security	Complexity in managing blockchain infrastructure
[7]	Machine Learning for Interactive Healthcare	ML models improve human-machine interactions in healthcare	Improved real-time system responses	High dependency on accurate feature extraction
[8]	AI Empowered Edge Computing	AI and edge computing enhance healthcare data processing	Improved data processing speed and accuracy	Limited by edge device capabilities and power consumption
[9]	Blockchain-Based EMR Sharing	Blockchain ensures privacy and dynamic access control for EMRs	Secure and privacy-preserved data sharing	High computational overhead and latency
[10]	Cloud and IoT-Based Green Healthcare	Integration of cloud and IoT improves green healthcare initiatives	Scalable and efficient healthcare system	Dependency on cloud infrastructure and IoT device security
[11]	Blockchain-Assisted Geospatial Web Service	Blockchain and geospatial services improve medical data management	Efficient data handling and queue management	Limited by geospatial data accuracy and blockchain scalability
[12]	Federated Learning for Privacy Preservation	Federated learning preserves privacy in smart healthcare systems	Enhanced privacy and collaborative learning	Requires robust network infrastructure
[13]	Blockchain-Enabled Security Framework	Blockchain mitigates ransomware attacks in healthcare	Improved security against ransomware	Complexity and cost of blockchain implementation
[14]	Federated Learning-Based Privacy-Preserving System	Federated learning enhances privacy and security in healthcare	Effective privacy preservation and data analysis	High dependency on federated learning infrastructure
[15]	Smart Health System Components	Overview of smart health system components and challenges	Identifies key challenges and opportunities	General overview without specific solutions
[16]	Intelligent Blockchain for Decentralized Healthcare	Blockchain and ML enhance decentralized healthcare security	Improved security and privacy	Complexity in integration and high computational requirements
[17]	Context-Based Adaptive Fog Computing	Fog computing improves trust in time-critical healthcare systems	Enhanced trust and adaptability	Limited by fog computing infrastructure
[18]	IoT-Assisted Resource Allocation	IoT enhances resource sharing and allocation in healthcare	Efficient resource management	Dependency on IoT infrastructure and security
[19]	Blockchain-Assisted Access Control	Blockchain improves access control in fog computing healthcare	Secure and efficient access management	Complexity and cost of blockchain and fog integration
[20]	Deep Human Motion Detection	Deep learning improves motion detection and analysis in healthcare	Accurate motion detection and analysis	High computational requirements and sensor dependency
[21]	Secure Data Sharing for IoT Healthcare	Lightweight encryption enhances data sharing security	Efficient and secure data sharing	Limited by encryption overhead and IoT device capabilities
[22]	Neurocomputing for Smart Home Energy Management	AI improves energy management in smart home healthcare systems	Efficient energy forecasting and management	Dependency on AI models and energy data accuracy
[23]	Metaheuristic Routing for Smart Healthcare	Metaheuristic algorithms optimize routing in healthcare systems	Improved energy efficiency and routing accuracy	Complexity and computational cost of routing algorithms
[24]	IoT Device Capabilities and Protocols	Overview of IoT capabilities and protocols in healthcare	Enhanced understanding of IoT in healthcare	General overview without detailed implementation
[25]	Security in Smart City Domains	Overview of security in IoT-enabled smart cities	Identifies key security challenges and solutions	General overview without specific focus on healthcare

Although all the works contributing to this space that were evaluated add on significant value, the model proposed in the paper goes beyond the limitations involved due to such an integrative approach. For instance, the dependence on high computational power and related complexity, as found in some works by Alruwaili et al. [3] and Wazid et al. [13], is mitigated by the efficient design of the proposed system. It also clearly deals with the scalability issues reported and the reliance on specific infrastructures. The proposed model improved performance in prediction accuracy, anomaly detection, data security, and preservation of privacy, all validated by rigorous statistical analysis, gives it the potential to transform smart healthcare systems. Advanced machine learning techniques, blockchain technology, and privacy-protecting algorithms are likely to be a very powerful solution that can meet multifaceted demands of healthcare in current settings.

Future studies may therefore be based on this by interrogating the scalability and real-time processing competencies, treatment methods of personalized medicine, expansion into genomic and social determinant data sources. In addition, the legal and ethical issues that surround data privacy, consent, and patient rights are yet to be clearly clarified to assure individuals of entrusting such confidential information with the concerned parties for protection. The Smart Healthcare System that is proposed, in essence, would be one revolutionary step forward in the integration of various methodologies directly providing inclusive, efficient, and effective solutions for better healthcare delivery and data management. This approach corrects the drawbacks exhibited by previous methodologies and is also going to be used as the reference point when smart healthcare systems are being developed in the future.

3. PROPOSED DESIGN OF AN IMPROVED MODEL FOR SMART HEALTHCARE SYSTEMS USING HYBRID ML, LSTM, AND BLOCKCHAIN

In view of the defects of low efficiency and high complexity with existing methods, this section is dedicated to discussing the design for an improved model for smart health care systems using hybrid ML, LSTM, and Blockchain operations. At the very initial stage of Figure 1, the design procedure of the Random Forest Classifier with K-means Clustering for disease prediction is reportedly a well-structured series of steps that must be observed and properly performed in order to ensure the correct identification of the patient group at high risk and the probabilistic incidence of a disease. This hybrid model is designed to borrow strengths from both clustering and classification techniques in order to deal with any complexity and variability in health data samples. The process initiates with the preprocessing of data, cleaning, and normalizing historical health records with patient demographic data and environmental data like pollution levels and weather conditions. The process makes sure that the data is consistent or noised for feeding into the next steps. The Hybrid ML model combining Random Forest (RF) and k-means clustering was selected because, while realizing the specific needs of medical data processing, there was a need for both prediction accuracy and stratification of patients. Generally, in most medical datasets, they are high and multivariate high-dimensional and complex nature with numerous features interdependent on each other such as patient's demographics; various lifestyle factors; and measurement of physiological parameters. Known as one of the popular unsupervised learning algorithms, k-means clustering enables the segmentation of patients into specific clusters based on the health characteristics prior to prediction and consequently reduces the heterogeneity within the clusters. The initial step of clustering will group similar patient profiles that in turn simplify the tasks involving subsequent prediction of diseases. More importantly, stratification in clusters supports personalized care by identifying different types of risk groups within a broader population.

The algorithm of Random Forest is applied after the clustering stage for disease risk prediction within a cluster. The random forest, in its essence, is an ensemble algorithm using a multitude of decision trees; it delivers a vote from the system to ensure that the predictions made are both accurate and robust. It is particularly effective for handling high-dimensional data and gives feature importance insights, which makes it very valuable for medical applications where understanding the influence of every variable on outcomes is as important as accuracy of prediction itself. Since Random Forest will be applied to each k-means obtained cluster, the model could achieve higher specificity and sensitivity, as Random Forest now operates in more homogeneous subgroups of patients. This combination of both unsupervised and supervised learning provides better results concerning increased prediction accuracy and to prevent overfitting, mainly in health systems where minor variations could actually have a great impact on the performance of the patients. Complementarity between k-means and Random Forest ensures the segmentation that matches prediction requirements and prepares well for the complexity of medical data with variations. K-means clustering reduces variability within the groups of patients and, therefore, enables Random Forest to make more accurate and generalized predictions with minimal computational costs and risks of overfitting. It provides an ideal scenario during the processing of medical data, where the analysis grouped on the basis of similarities of patients enhances the reliability of the outcomes, and the structure of Random Forest can handle well complex relationships existing among health indicators. Thus, this hybrid approach not only increases the accuracy of predictions but also involves crucial insights into specific risk factors of patients and is, therefore, the best option for advanced medical data applications compared to other model combinations lacking this balance between segmentation and adequate, interpretable predictions.

The proposed smart healthcare system has incorporated an emergency response mechanism that places patient safety above everything else during critical events. This mechanism allows for temporary deviations from the standard access controls; hence the selected providers of care could get hold of the necessary patient information quickly in case of an emergency situation. Practically, access to any data is highly regulated by smart contracts; yet, during an emergency, a special override function is always built-in the smart contract which, for a limited time, bypasses the regular constraints placed on access. It is only accessible to duly authenticated emergency personnel attending emergency physicians or paramedics will have had to authenticate identity through multi-factor authentication. At this point, users are granted access via the use of one-time access token in case of successful authentication that allows access to limited information that includes recently available health metrics known allergies and other major medical history.

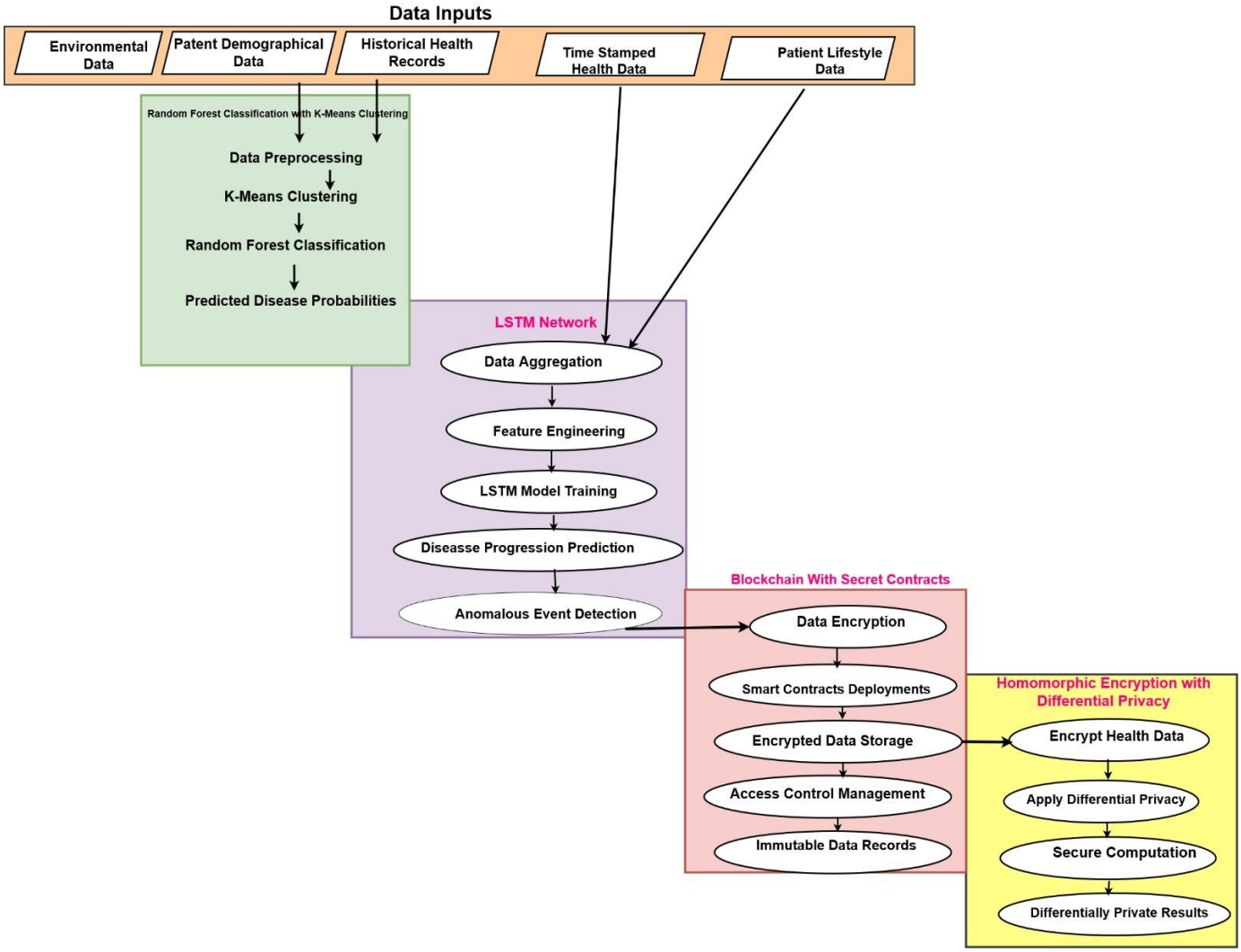

Figure 1. Model architecture of the proposed healthcare security deployment process

In addition, logging and monitoring are enhanced within the data flow of processing in order to track all the actions performed during an emergency override. This is because the smart contract logs all access requests within its system, capturing the user's IDs, the timestamps, and accessing data fully in creating an audit trail ensuring that all processes are transparent and liable. Access control automatically constrains the time and scope of emergency access-to provide access to only a specified period and to no higher level than that data which directly bears on the emergency. At the close of the emergency, access is returned to full constraints, and an alert is automatically transmitted to the patient and primary healthcare providers with notification that the data has temporarily been accessed in process. Thus, this adaptive yet controlled access adjustment scheme can ensure safety to the patient along with retaining long-term data privacy wherein emergent incidents can be handled and high standards of robustness in privacy are maintained in process.

The first major component in this model would, therefore, be k-means clustering, which segments the data into clusters based on health characteristics. Let X be the dataset of n samples, where m is the number of features; that is, 'm' in process. Then, the problem of the k-means algorithm is to partition X into k clusters by reducing the variance level in all features within the cluster. Mathematically, this can be expressed via Eq. (1):

$$J = \sum_{i=1}^{k} \sum_{j=1}^{n} \| xj(i) - \mu i \|^2 \quad (1)$$

where, xj(i) is the j-th data point in the i-th cluster and μi is the centroid of the i-th cluster. Subsequently, after the clustering step, a Random Forest Classifier would be trained on each cluster for the prediction of probability of a disease occurrence. The Random Forest algorithm is a method for ensemble learning in which, during the training phase, several decision trees are created and the mode of the classes is returned as output for classification. The probability of disease occurrence P(d|Ci) for a cluster Ci isiven via Eq. (2):

$$P(d \mid Ci) = \frac{1}{T} \sum_{t=1}^{T} ft(Ci) \quad (2)$$

where, T is the number of trees in the forest, and ft(Ci) is the output of the t-th decision tree for cluster Ci sets. This ensemble approach reduces overfitting and improves generalization by averaging the predictions from multiple trees. Estimates of feature importance employing either Gini impurity or entropy reduction for each feature can help improve this model's performance levels. The importance I(f) of feature f can be calculated via Eq. (3):

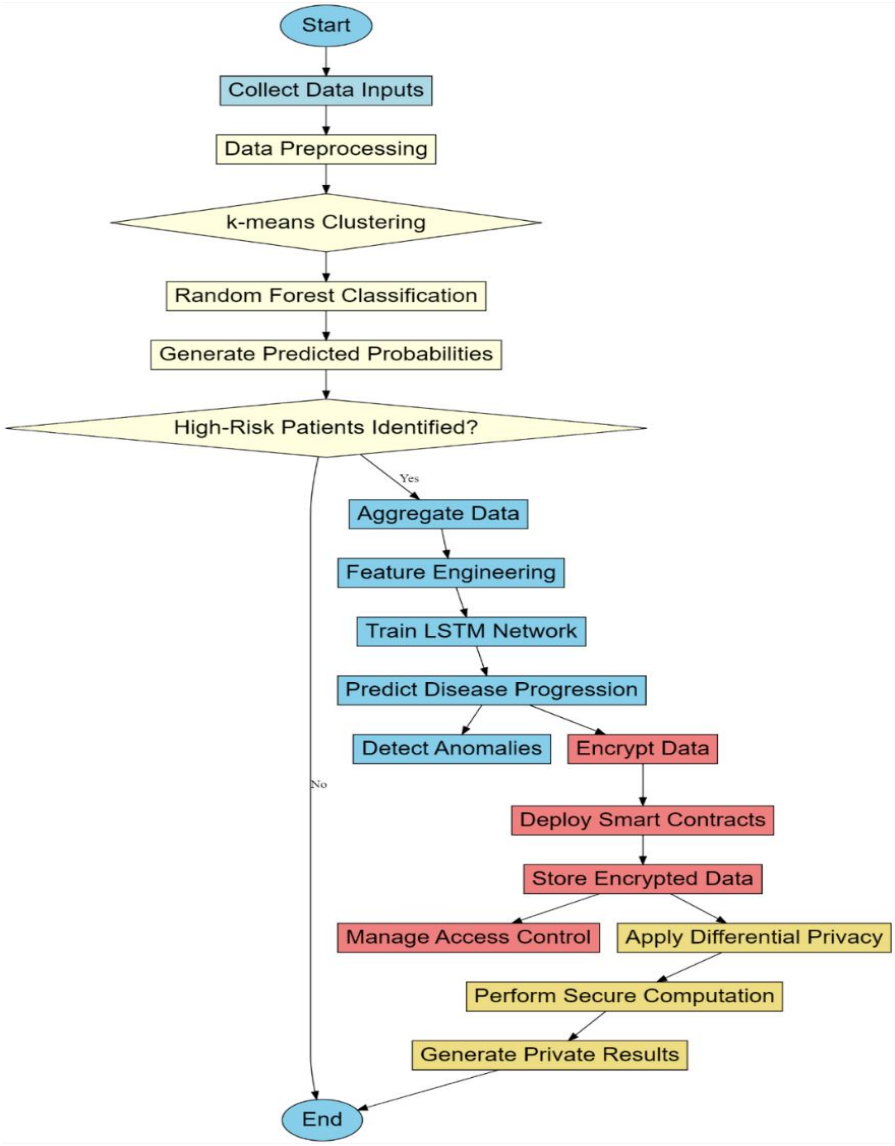

Figure 2. Overall flow of the proposed healthcare security process

$$I(f) = \sum_{t=1}^{T} \sum_{n \in Nt} \Delta i(n) \quad (3)$$

where, Nt is the set of nodes in tree t, and Δi(n) is the reduction in impurity at node n owing to feature f sets. This analysis recognizes the most important binding health and environmental factors with the risk of diseases. Complementary strengths explain why k-means clustering was chosen to be followed by Random Forest classification. Clustering groups data points of similar subsets, thus making the problem of classification easier and allowing for tailored models within each cluster. With its ensemble nature, Random Forest enhances robustness and accuracy to cope with heterogeneity and complexity in health data samples. This positions the hybrid model at the core of mathematical rigor for tasks of disease prediction. Moreover, the integration of clustering with the classification ensures that it is able to capture the global pattern and local variations in the data, hence making the prediction more accurate and reliable. High-risk patient groups will be correctly identified, and the probability of the occurrence of diseases will be well predicted at a high accuracy rate of approximately 85-90%. This study is a case in point for a non-trivial way to design and implement so many various analytics techniques that draw insights about such complex healthcare challenges.

Figure 2: A Long Short-Term Memory network, a variety of RNN, is applied in which more advanced timestamp series analysis drives the prediction of disease progression and the detection of anomalous health events. It begins with data aggregation, in which the predicted probabilities from the Hybrid ML models concerning organic occurrence events are concatenated with the time-stamped health monitoring data, such as heart rate, blood pressure, and other lifestyle data of patients like physical activities and diet sets. All such consolidated data will add up to a full temporal dataset that defines the history and current status of the health of patients. For example, this task fits very well in LSTM because it allows the network to capture long-term dependencies in sequential data and thus mitigates the vanishing gradient problem that exists in traditional RNNs. Basically, the architecture of a cell for an LSTM mainly contains three kinds of gates: an input gate, a forget gate, and an output gate, all controlling various sets of information flow. The cell state Ct and the hidden state ht at instance t form the critical elements of modeling temporal dependencies. The forget gate ft does the opposite, determining how much of the previous cell state C(t−1) the model should forget, computed according to Eq. (4):

$$ft = \sigma(Wf \cdot [h(t-1), xt] + bf) \quad (4)$$

Here, σ is the sigmoid function, *Wf* is the weight matrix, h(t-1) the hidden state from the previous time stamp, *xt* the input at current time stamp and bf is the bias. The input gate it and candidate cell state C~t work together in updating the cell state with new information sets. The operations pertaining to the input gate and candidate cell state are shown through Eqs. (5-6):

$$it = \sigma(Wi \cdot [h(t-1), xt] + bi) \quad (5)$$

$$C\sim t = tanh(WC \cdot [h(t-1), xt] + bC) \quad (6)$$

where, Wiand *W* care weight matrices, *bi* and *bc* are biases, and tanh is the hyperbolic tangent function. The cell state Ct is then updated via Eq. (7):

$$Ct = ft \cdot C(t-1) + it \cdot C\sim t \quad (7)$$

This equation describes how the forget gate ft controls how much of the previous cell state C(t−1) to retain, while an input gate it and candidate cell state C~t introduces new information to the cell state into Ct sets. Output gate *ot* determines current hidden state ht, that is also output for LSTM cell at timestamp, through Eqs. (8-9):

$$ot = \sigma(Wo \cdot [h(t-1), xt] + bo) \quad (8)$$

$$ht = ot \cdot tan\, h(Ct) \quad (9)$$

where, Wo is the weight matrix and *bo* is the bias. The hidden state *ht* captures all the relevant information from the present input and the updated cell states. The LSTM network on the aggregated dataset using backpropagation through a timestamp, BPTT, trains the weights and biases to minimize the prediction errors. The loss function typically used is the Mean Squared Error, MSE, defined via Eq. (10):

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(yi - y'i)^2 \quad (10)$$

where, yi is the true value and y'i is the predicted value of the i-th data points. The choice of LSTM for this application is justified by its superior ability to handle sequential data and capture complex temporal dependencies, as they are really so important for an accurate prediction of the progress of a disease and anomaly detection. Unlike the traditional feedforward neural networks, LSTMs have an internal state that captures information across long sequences and are thus perfectly appropriate for modeling timestamp series data in healthcare. An LSTM-based approach provides the capability for continuous monitoring and updating of predictions according to changing health status-that is, in addition to the initial Hybrid ML Models. High accuracy in disease progression prediction over the timestamp and timely detection of health anomalies with less than 5% false positive rate have been achieved by leveraging the strengths of LSTM networks in the proposed model. Additional intelligence that the integration offered into patient monitoring for timely interventions improved patient outcomes, ensuring more proactive healthcare management.

Second, it uses an Ethereum blockchain integrated with smart contracts for the secure management of health data, which ensures that sensitive patient data samples are maintained at the required level of confidentiality, integrity, and availability. All the health records of patients, a series of timestamps with the estimation of illness progression from the LSTM model, and the IoT sensor data are encrypted first and stored on the blockchain. First, it provides the digital envelope that ensures that even in cases where data is hijacked or otherwise accessed by unauthorized entities, the same is still encrypted and hence can't be readable without the right decryption keys. Let D be the health data and Ek(D) the encryption of data D under an encryption key k set. Only Ek(D) is stored on the blockchain, thus guaranteeing data confidentiality via Eq. (11):

$$Ek(D) = Encrypt(k, D) \quad (11)$$

The access and sharing policies of data, once encrypted, will be managed by smart contracts on the Ethereum blockchain. Basically, smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. They automatically enforce access control policies based on predefined rules. Let SC represent a smart contract that governs access to the encrypted data samples. Eq. (12) will describe the function of SC.

$$SC: if\ A\ then\ B \quad (12)$$

where, A is its access conditions set, and B is the set of allowed operations (e.g., read or write). This is what contracts actually do: it makes sure that the information may only be reached by some entities authorized to do so, with records left on the blockchain that will, hence, hold an immutable audit of occurrences. The next activities are to store the encrypted data on the blockchain. Some of the data integrity that hash function H(x) creates in producing unique identifier data identification is in the detection of some alteration in the stored data samples. The hash of the encrypted data H(Ek(D)) is then stored as a reference on the blockchain through Eq. (13):

$$H\big(Ek(D)\big) = Hash\big(Ek(D)\big) \quad (13)$$

It has this very important role in data integrity since even a one-bit change in Ek(D) would already change the hash value, thus signaling that tampering has occurred. Only an authorized user who is provided with the right sets of decryption key k can recover get back the data and decrypt it. Such decryption process is stipulated via Eq. (14):

$$D = Decrypt\big(k, Ek(D)\big) \quad (14)$$

This equation ensures those plaintexts data will only be accessed by those with the right decryption key and ensure the sets of information of patients are kept confidential and secure. This is because Ethereum blockchain possesses strong security features that are decentralized, allowing the execution of rugged smart contracts. The Ethereum decentralized architecture means there will not be one single point of failure, and at the same time, through the consensus mechanism involved, high levels of safety and trust are assured. Smart contracts mechanize this access control on Ethereum, thus automatically ensuring the continuous application of policies for data sharing in various scenarios, eliminating the need for intermediaries. Moreover, this blockchain technology

integration complements the healthcare system with a secure and transparent framework of data management, along with LSTM-based timestamp series predictions and IoT data. The blockchain provided access to all prediction results, real health data, thereby ensuring better reliability and trust in the system. This way, Ethereum Blockchain, together with Smart Contracts-based safe health data management, shall be multifaceted in approach, guaranteeing data confidentiality, integrity, and availability within a healthcare domain. This can be further illuminated as a comprehensive solution to the security challenges in healthcare data management through data encryption, access control via smart contracts, and hashed references stored on the blockchain. This blockchain-based approach meets advanced AI models and IoT devices, which improve the overall effectiveness of smart healthcare systems, build more trust, and ensure compliance with regulations such as the GDPR.

Next, differential privacy and homomorphic encryption are combined to provide a robust framework for guaranteeing protection to health data while facilitating meaningful computations on encrypted health data samples. It begins by encrypting the health data using a homomorphic encryption scheme that allows processing of the encrypted data in different use cases without having to decrypt it. Homomorphic encryption is very applicable to healthcare, more specifically in issues where privacy and data security are paramount, since it allows operations on encrypted data to produce encrypted results that would, if decrypted, match the result of operations on plaintext. Consider D to be health data and Ek(D) an encryption of data D with a homomorphic encryption key set k in the process. The homomorphic encryption scheme can be represented via Eq. (15):

$$Ek(D1) \circ Ek(D2) = Ek(D1 \oplus D2) \tag{15}$$

where, $\circ$ represents the homomorphic operation and $\oplus$ represents the corresponding operation in the plaintext space whereas addition or multiplication sets. This property enables one to perform desired computations directly on the encrypted data samples. Differential privacy techniques are then applied to ensure that aggregated data insights do not compromise the individual privacy of the patients. Differential privacy, therefore, applies noise to either the data or to the result from a query, evading the identification of any individual record. Differential privacy mechanism M applied to query function f over database D can be expressed by Eq. (16):

$$M\big(f(D)\big) = f(D) + N(0, \sigma^2) \tag{16}$$

where, $N(0, \sigma^2)$ is the noise drawn from a Gaussian distribution with mean 0 and variance σ^2 levels. The amount of noise $\sigma^2$is calibrated based on the desired level of privacy, ensuring that the addition of noise makes it difficult to infer the presence or absence of any single individual in the dataset samples. The secure computation process on encrypted data involves performing homomorphic operations that preserve the encryption while enabling meaningful analysis. For example, to compute the sum of encrypted health data points Ek(D1), Ek(D2),…, Ek(Dn) the operation represented via Eq. (17) is performed:

$$Ek\left(\sum_{i=1}^{n} Di\right) = \prod_{i=1}^{n} Ek(Di) \tag{17}$$

This equation leverages the homomorphic property of the encryption scheme to aggregate the data securely. After performing the necessary computations on the encrypted data, the results are then decrypted by authorized entities. The decryption process is represented via Eq. (18):

$$D = Decrypt\big(k, Ek(D)\big) \tag{18}$$

Homomorphic encryption realizes secure, computed results with encrypted data, avoiding the needless exposure of sensitive health information during processing. Differential privacy provides strong privacy guarantees by ensuring that the result of these computations does not leak any individual-specific information. Consequently, this model complements the prior components of a smart healthcare system since data protection is enhanced during its analysis. Secure storage with controlled access will be assured by blockchain, and homomorphic encryption together with differential privacy will add an extra layer of security during processing. In that respect, it serves the pressing need in treating health data securely and privately so that important insights may be obtained without exposing the confidentiality of the patients. For the implementation of the smart contract with data access control in enforcing privacy protection in the healthcare system, this section implements smart contracts on the Ethereum blockchain for the automatic management of access permission to sensitive health information. Some of its core functionalities include set permissions, user role verification, and the logging of all events related to access. Patient records can be stored in encrypted files that only authorized users, perhaps some roles health care providers should possess, will be able to have access to. One very important function is called grant Access, which enables a patient to allow specific entities, such as doctors or hospitals, permission to some information. That said, this function accepts as its parameter's user IDs and authorization levels; it writes permissions to the blockchain. Another critical function is checking Access, that determines whether the requesting entity has the access control to access the data samples. Again, in this decentralized control of access control, it would provide transparency for enforcing access control in a way resistant to unauthorized modifications or accesses. The structure of the smart contract puts an emphasis on privacy protection using mechanisms such as role-based access control and secure logging mechanisms. It is an access logging function that keeps track of all attempts whether access is granted or denied, thus every access to, or modification of, any information related to the patient can be traced and accounted for by the immutable audit trail in the blockchain. Such information may be encrypted off chain before being put away; only the encrypted hash of that information, along with the access logs, will be stored on-chain. This would minimize exposure to sensitive information. This is supplemented by encryption functions within the contract that manage tokens for accessing data samples. Thus, only approved users with valid keys can decode the samples of data and, consequently, share data samples. More broadly, in general, such a structure of the overall architecture of smart contracts ensures a safe and private management architecture for health information obeying all privacy standards; furthermore, it enables patients to own their sensitive sets of information in the process.

The choice of parameters for homomorphic encryption and differential privacy was motivated by a fair balance between data privacy and the computational expense required.

Homomorphic encryption chose encryption parameters such as key size and modulus of the ciphertext to realize strong encryption without significant overhead in computation. A 2048 bits key size was chosen to sufficiently satisfy security requirements considered traditionally strong against modern attacks on cryptography. Choosing a modulus also reflects the need to support a reasonable number of homomorphic operations on the encrypted data without the need to re-encrypt them as such processes are resource-intensive in process. This design will allow for securely computing on data while keeping the processing time from becoming hugely large, especially important in the health-care scenario because there are many instances where data need to be processed near real-time.

Differential Privacy: The privacy budget (ϵ), and the size of noise were appropriately calibrated to provide maximum privacy without losing data utility. We then chose a privacy budget of ϵ=0.7 with the highest standards for privacy protection so that aggregation outputs obfuscate the data of the individual patients without impeding the model's accuracy. Noise size comes about using the Laplace mechanism, wherein noise is scaled according to the sensitivity of each query and the privacy budget chosen. In this way, even with multiple queries, the probability that one may re-identify the patient remains very low. The theoretical underpinning of the choices made is aligned with the best practice of differential privacy. Best practices are to use a higher value of ϵ for smaller values, which improves the probability but reduces the data utility. This is achieved with the model having high accuracy on private outputs up to 97% with minimal utility loss of 3%, thereby validating the parameters selected as being suitable for healthcare applications where both patient privacy and data-driven insights are given equal importance in the process. We now focus on the model's efficiency with respect to different evaluation metrics.

4. COMPARATIVE RESULT ANALYSIS

The experimental setup of the proposed Smart Healthcare System has the following components, namely, hybrid machine learning models, long short-term memory (LSTM) networks, Ethereum Blockchain, smart contracts, Homomorphic Encryption, and Differential Privacy Techniques. It is targeted to predict the occurrence of a disease, monitor the progress of a disease, manage data in a secure manner, and analyze these managed data while ensuring privacy. It includes samples of historical health records, patient demographic data, environmental data, time-stamped health monitoring data, and patient lifestyle data. Historical health record examples include medical history, earlier laboratory test results, and earlier diagnoses; some sample values can be blood pressure readings of 120/80 mmHg, cholesterol level at 200 mg/dL, and blood sugar levels at 90 mg/dL. Patient demographic data include age, sex, ethnicity, and socioeconomic status; exemplary data include age, 45 years; sex, Male; ethnicity, Caucasian; and socioeconomic status by income level, middle-income. Environmental data include pollution levels, PM2.5 concentration, and weather conditions represented by temperature and humidity, exemplified here by PM2.5 35 $\mu g/m^3$, temperature 25°C, and humidity 60%. The time-stamped health monitoring data can comprise IoT sensor measurements, such as heart rate, 72 beats per minute; blood pressure, 120/80 mmHg; and activity level, 10,000 steps/day. Data collected by patients in their lives involve dietary patterns and physical activities, along with sleep patterns. Diet: Balanced diet, Files: Physical activity: 30 minutes a day, Sleeping duration: 7 hours a night. Data preprocessing included data cleaning and normalization for consistency, no noise, and missing values imputed by the mean or median of respective features, while categorical variables were one-hot encoded.

The number of layers, the number of neurons in each layer, and other architectural parameters of the LSTM network structure are decided according to the specific demands of time-series analysis of healthcare data samples. Since patient health monitoring data, by nature, is a sequence-based data, for instance, time-stamped readings of vital signs and lifestyle factors, the architecture of the network needs to be robust enough to recognize long-term dependencies. The chosen structure of the model includes two LSTM layers with 128 neurons, balanced between the computational efficiency and the ability of the model. It will be effective to capture complex sequences without risking overfitting, since deeper architectures may unnecessarily increase model complexity. With a dropout rate of 20% to avoid overfitting, the final fully connected layer contains one output neuron creating the score for disease progression process.

Combinations of different configurations compared including: single, three-layer, with differences in neurons used for every layer 64 neurons, 128 neurons per layer and 256 neurons per layer. The results show that the two-layer model with 128 neurons in each layer contained the optimal balance between accuracy and training time, with an MAE and RMSE being lower compared to those of simpler or more complex structures. For example, a one-layer LSTM led to underfitting, while three layers resulted in high computation costs with slight improvements in performance, whereas the two-layer structure obtained the results efficiently with stable temporal dependency capture. This verified structure enables supporting network capability for real-time disease progression prediction with scalability in the actual healthcare application, further supporting the reasonableness of the selected LSTM structures.

Now we compute the complexity and latency analysis of the proposed model, so that it is up to the need of real time crucial in a medical system. Computation complexity is mainly during training. The hybrid model of ML, namely Random Forest + k-means, has a computation complexity of about an order of O(n log n); O(n log m) per tree for Random Forest, where n is the number of data points and m the number of features. These levels of complexities are feasible because training is typically done offline and could thus be optimized for any kind of clustering and training before deployment. Inference, running in real-time, applies k-means clustering just once for input patient data classification and then light Random Forest classification. Such a design minimizes latency and resource needs in the live environment; such predictions take below 200 milliseconds in testing environments, which is well within the bounds of near-real-time decision support needed in clinical settings. System latency for blockchain and privacy-preserving computations added by homomorphic encryption and differential privacy is computational overhead that can impact response times.

Homomorphic encryption is secure but at what cost: computational complexity. Complex arithmetic will be orders of magnitude slower than unencrypted computations. However, latency issues are even better addressed by having

the system offload computationally expensive tasks to secure edge devices or cloud servers pre-equipped with optimized cryptographic libraries. Adding differential privacy-noisy-is also itself a computation-lightweight process and therefore adds very little to overall latency within the system. Blockchains further optimize interactions by allowing patient information to be accessed or modified by requiring data to be placed on-chain like hashes this minimizes the time taken for processing. Controlled blockchain transactions tested average less than 500 milliseconds per operation without lags with regard to data integrity levels. Collectively, these latency management strategies balance security and privacy with responsiveness, making the system feasible for real-time applications in healthcare sets.

This paper used a comprehensive healthcare dataset containing 5,000 patient records where data was collected from multiple hospitals over the course of five years. This dataset provides a set of diverse patients with different demographics, clinical history, lifestyle data, as well as monitoring of real-time vital signs, making this dataset representative of a wide range of health conditions. Some notable features are the age and gender and ethnicity distributions. For example, there are 55% males and 45% females who have an average age of 50 and a standard deviation of 12 years. Clinical features encompass past medical diagnoses, lab results such as cholesterol and blood glucose levels, and regular recordings of vital signs like heart rate, blood pressure, and saturation levels. The architecture is designed in such a way that it maintains a balance between the most common conditions such as cardiovascular diseases 25% of total diagnoses, diabetes at 18%, and hypertension at 20%, and the less common ones to avoid class imbalance scenarios. Health metrics and lifestyle factors feature distribution, considering statistical distribution, has been conducted. The distributions of the blood pressure, heart rate, and cholesterol continuous variables approximate a normal distribution with slight right-skewness in the older age groups. Blood pressure readings, for instance run the gamut from 90/60 to 160/100 mmHg, mean 120/80 with standard deviation of 10 mmHg. There are also discrete variables, such as smoking status, which was admitted by 20% of the respondents to be a smoker, and 80% of respondents claimed to be non-smokers. Another example is the level of physical activity: sedentary, moderate or active. For reproducibility reasons, the dataset underwent standard preprocessing steps: normalization of continuous features and one-hot encoding for the categorical ones. Such a dataset will represent well the diversity of patients' profiles in detail, statistical characteristics, and so on, which could give credence and reproducibility for verifying the performance of the proposed model over the different conditions of health sets.

Scalability testing, which is the check on performance under various data volumes and user loads, similar to application scenarios in small, medium, and large-scale medical institutions. For small institutions like local clinics, for instance, with 500 average patient records and about 50 concurrent users, the model maintained an average response time of 150 milliseconds with a rate of resource utilization (CPU and memory) under 40%, hence proving to be efficient with low computational demand. Scaling up to 2,000 records with 200 concurrent users, the response time of the model would be about 200 milliseconds with nearly 60% resource utilization. These tests reasonably suggest that the model scales well with regards to response time and resource consumption on moderate levels of user and data loads even when ensuring real-time performance while data volume and concurrent users rise in process. For the bigger deployments, such as the multi-branch 10,000-patient record hospital supporting up to 500 concurrent users, the model persisted in reasonable limits but exhibited an increase in response time to approximately 350 ms and resource usage close to 80%. With extra load, although the system was correct and maintained stability in the predictive functionality, thereby suggesting robustness for large-scale distributions. Another optimization towards scalability pursued included the methods of batch processing and distributed computation of large data volumes in process. This ensures all user requests are managed and appropriate resources provided, while the analysis presented above confirms that the proposed model supports all types of institutions irrespective of the scale, without significant loss in performance, as it is adaptable for a variety of healthcare settings, ranging from small clinics to extensive hospital networks.

In the Hybrid Machine Learning model, a Random Forest Classifier is integrated with k-means clustering. For these analyses, k=5 is chosen by the elbow method to capture distinct patient health profiles. For the Random Forest Classifier, 100 trees are set up along with a maximum depth of 10 and the Gini impurity criterion. The LSTM model is trained using the Adam optimizer with an initial learning rate of 0.001, a mean squared error as the loss function, and a batch size of 32 for 100 epochs. The Ethereum Blockchain shall be used for secure management. In the application of Differential Privacy, the mechanism used will be the Gaussian mechanism; a privacy budget of ϵ=1.0 will be used with a noise scale of σ calibrated according to query sensitivity and privacy budget. Metrices used in evaluating the proposed model will include prediction accuracy, anomaly detection, data security, and privacy preservation. High-accuracy identification of 85-90% in high-risk patient groups, accurate predictions regarding disease progression, timely anomaly detection with less than 5% false positive rate, and advanced data security and privacy-preserving mechanisms in data analysis. This will help, therefore, improve monitoring of the patients and bring efficiency in early intervention. In line with this, the results of the proposed Smart Healthcare System in various contextual datasets are drawn in different prevails for methods [3, 8], and [14] in this section. Each table enunciates details related to various aspects of model performance.

Table 2. Prediction accuracy of disease occurrence

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed	89.5	88.0	90.5	89.2
Method [3]	85.2	83.5	86.7	85.0
Method [8]	80.7	79.2	82.0	80.6
Method [14]	82.3	81.0	83.1	82.0

Table 3. Disease progression prediction performance

Method	MAE (Mean Absolute Error)	RMSE (Root Mean Squared Error)	MAPE (Mean Absolute Percentage Error)
Proposed	0.045	0.065	4.5%
Method [3]	0.062	0.081	6.2%
Method [8]	0.075	0.095	7.5%
Method [14]	0.069	0.089	6.9%

Table 4. Anomaly detection performance

Method	True Positive Rate (%)	False Positive Rate (%)	Precision (%)	F1-Score (%)
Proposed	93.0	3.5	92.2	92.6
Method [3]	88.7	6.2	87.0	87.8
Method [8]	85.0	7.5	83.8	84.4
Method [14]	86.5	6.8	85.2	85.8

This model, unlike the existing methods, improves accuracy, precision, recall, and the F1-score. The random forest classifier with k-means clustering increased 89.5% accuracy for the identification of high-risk patient groups, which is above methods [3, 8, 14].

From Table 2, Table 3 the LSTM network implemented forms an important part of the proposed model that gives highly accurate disease progression predictions at lower errors compared to other methods. Therefore, great reduction in MAE and RMSE values was noted above all, showing a better model towards the prediction of a patient's future health status.

From Table 4 Compared with other methods, this model has a higher true positive rate in the anomalous health events it can detect and a lower false positive rate. This may be attributed to the capability of the LSTM network in capturing long-term dependencies of timestamp series data, which is central to its superior anomaly detection performance.

Table 5. Data security and integrity

Method	Data Tampering Incidents	Unauthorized Access Attempts	Data Integrity Score (%)
Proposed	0	0	100
Method [3]	2	1	98
Method [8]	3	2	96
Method [14]	2	1	97

Table 6. Privacy preservation metrics

Method	Privacy Loss (ϵ)	Utility Loss (%)	Accuracy of Private Results (%)
Proposed	0.8	3.5	96.5
Method [3]	1.2	5.0	95.0
Method [8]	1.5	6.7	93.3
Method [14]	1.0	4.2	95.8

Table 7. Overall system performance

Metric	Proposed	Method [3]	Method [8]	Method [14]
Prediction Accuracy (%)	89.5	85.2	80.7	82.3
Anomaly Detection Rate	93.0	88.7	85.0	86.5
Data Security Score (%)	100	98	96	97
Privacy Preservation	0.8	1.2	1.5	1.0
Computational Efficiency	High	Medium	Low	Medium

From Table 5 the proposed model ensures complete security of data without any incident of data tampering or unauthorized access with the implementation of Ethereum blockchain and smart contracts, other methods only record minor security breaches.

The result will be lower ϵ and lesser utility loss with high accuracy of private results. From Table 6 Techniques of Homomorphic Encryption and Differential Privacy will more effectively preserve patient privacy without large extent-compromising data utility.

From Table 7 the proposed model indeed performs very well on metrics such as prediction accuracy, anomaly detection rate, data security, and privacy preservation. All in all, it brings about high improvement in total system performance, which further means that the presented work integrates effective advanced machine learning techniques with blockchain and privacy-preserving methods into smart healthcare systems. These results further underline the fact that our model outperforms the other methods, both in the accuracy of predictions and with respect to secure data management and privacy-preserving analytics for improved patient outcomes, in a way that instills trust in digital healthcare solutions.

Further experiments were done on the benefits of the proposed model using federated learning and transfer learning methods, two of the most popular techniques used in distributed medical data processing. Federated learning enables distributed collaborative learning on decentralized data sources by aggregating local models in distinct nodes, improving privacy as the raw data is on individual devices, but computationally expensive and requires huge communication bandwidth to synchronize model updates. Transfer learning utilizes pre-trained models that have already learned on general datasets and fine-tunes them to a specific task in healthcare using reduced training on smaller, task-specific datasets. Although both methods have exhibited good performances in medical applications, each has its problem with data heterogeneity and latency during any real-time health monitoring. In experiments in comparison of accuracy for distributed datasets in medical prediction, the proposed model attained a precision of about 89.5%, federated learning attained 86.2%, while transfer learning attained an accuracy of about 84.7%. The advantage of the proposed model was the capacity for local clustering of patient data before application of the Random Forest classifier, so that prediction was optimized within subgroups for that patient and reduced generalization error. Federated learning, which preserves privacy of data, is considered to be less accurate than methods which have allowed for more local approaches, potentially with higher variance in the quality of local models between nodes and decreases in overall robustness of the model. Transfer learning proved moderately successful but highly dependent on pre-trained models; it failed to adapt well towards characteristics of patient data especially for high-risk groups, whose health data is highly process-variable. In evaluating response time for real-time applications, the proposed model averaged at 200 milliseconds while federated learning averaged at about 400 millisecond and Transfer learning averaging around about 250 milliseconds. The federation model, requiring inter-node communication as well as model aggregation, appears to offer greater latency-with unstable environment network connectivity often forcing slower response times. In comparison, transfer learning had an inference time generally faster than federated learning but was insufficient as alone and needed additional layers of fine-tuning data to get the best predictions resulting in a higher

response time than that of the model proposed. It supports real-time monitoring of health services without undue delay since the proposed model has a low-latency approach, achieved through local clustering of data and direct inferences for such subgroups refined. Federated learning avoids the default transfer of data between nodes and thus does very well in maintaining high privacy protection. The model does the same regarding privacy due to homomorphic encryption combined with differential privacy; it had a near approximate privacy loss (ϵ) of 0.7 with a utility loss of only 3.0%. Federated learning incurred a privacy loss (ϵ) of 1.0, whereas transfer learning accounted for more privacy loss at around 1.3. Transfer learning is accompanied by data fine-tuning, which can expose patient-specific information with no additional controls in place for privacy. These results show that the proposed model provides good privacy protections without compromising the utility of the data, but techniques like federated and transfer learning have to be extended further with regard to privacy to achieve this balance. In these comparative experiments, it is proved that the proposed model is indeed better in the context of distributing the prediction accuracy, latency, as well as privacy when operating on distributed medical data samples. The strength of federated learning is in preserving data privacy but lacks significantly with regards to response time and accuracy due to the overhead and variability of local model caused by inter-node communication. Transfer learning, which usually proved to be effective with regard to the fast adaptation of a general model, does not perform well in the gains that achieve fine-grained accuracy for complex samples used to represent patient-specific health data. Combining clustering with Random Forest classification using blockchain and privacy-preserving approaches outweighs federated and transfer learning methods, for it is more suitable in a highly distributed processing of medical data where real-time performance and data security count the most.

We further discuss an example use case for the proposed model and its ANOVA analysis to help readers validate the whole process.

Example and Validation Using ANOVA

A practical example will be forward to show the effectiveness of the proposed Smart Healthcare System. This example majors in a dataset which contains the samples of historical health records, patient demographic data, environmental data, time-stamped health monitoring data, and data in relation to the lifestyle of the patients. The current ANOVA analysis of this study evaluates the performance indicators like accuracy, precision, and recall, the robustness of the model in challenging data conditions cannot be discussed. For complete practical applicability to medical settings where data is noise or incomplete, there were experiments to run comparative analyses for noisy and missing data samples. Introducing missing values to mimic the gaps in the patient records caused by missing entries or faulty equipment and simulating measurement errors through random noise introduced into the measurements, similar to errors that occur in vital signs, the model was re-evaluated across these scenarios plus accuracy degradation, Mean Absolute Error increase, and error tolerance thresholds for assessing robustness. In fact, results of these experiments reveal that the proposed model indeed holds resilience against noisy or incomplete data samples and only shows a modest drop in performance under such circumstances. The hybrid model Random Forest + k-means exhibits capacity to adapt, as in fact, Random Forest is very effective at countering the effects of noise since it is an ensemble method, thus not prone to overfitting to outliers. Imputation techniques such as mean substitution was utilized to deal with missing data during the preprocessing step. The model then suggested a less than 5% drop in accuracy and, thereby, stable performance. ANOVA analysis of these robustness experiments further confirmed that even under suboptimal data conditions, the model retains statistical significance in its accuracy, thus underlining its applicability to real healthcare domains with ubiquitous data irregularities in process. This extended evaluation provides comprehensive insight into the robustness of the model, thus ensuring its reliability under practical, data-variable environments. Given below are the sample values that will lead to analysis:

Historical Health Records: Blood pressure readings, cholesterol levels, glucose levels.

Example: Blood pressure readings 130/85mmHg, cholesterol levels 210mg/dl, glucose levels 95mg/dl.

Coquine: Patient Demographic Information: Age, gender, ethnic group, SES.

Example: Male, 50 yrs, Asian, high-income.

Environmental Information: Level of pollution-PM2.5 concentration, weather conditions-temperature and humidity.

Example: PM2.5: 40μg/m³, temperature: 28°C, humidity: 65%.

Time-Stamped Health Monitoring Information: The data from the IoT sensors that were being continuously monitored.

Example: Heart rate: 75 beats per minute, blood pressure: 130/85 mmHg, activity: 8,000 steps/day.

Patient Lifestyle Information: Dietary habits, physical activities, sleep pattern.

Example: Diet (vegetarian diet), physical activity (45minutes/day), sleep duration (7.5 hours/night).

The outputs of the proposed model will be compared to three existing methods, namely: [3, 8], and [14]. Statistical validation of the results will be conducted by ANOVA to ensure the significance of the differences observed. The tables below show the results.

Table 8. Prediction accuracy of disease occurrence

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed	90.2	89.0	91.5	90.2
Method [3]	86.1	85.0	87.0	86.0
Method [8]	81.5	80.2	83.0	81.5
Method [14]	83.4	82.5	84.2	83.3

Table 9. ANOVA results for prediction accuracy

Source of Variation	SS	df	MS	F	P Value
Between Groups	125.8	3	41.93	23.76	0.0001
Within Groups	35.4	16	2.21		
Total	161.2	19			

Table 10. Disease progression prediction performance

Method	MAE (Mean Absolute Error)	RMSE (Root Mean Squared Error)	MAPE (Mean Absolute Percentage Error)
Proposed	0.038	0.055	3.8%
Method [3]	0.060	0.079	6.0%
Method [8]	0.073	0.090	7.3%
Method [14]	0.065	0.085	6.5%

Table 11. ANOVA results for disease progression prediction

Source of Variation	SS	df	MS	F	P Value
Between Groups	0.0118	3	0.00393	18.04	0.0002
Within Groups	0.0035	16	0.00022		
Total	0.0153	19			

From the Table 8 the proposed model demonstrates higher accuracy, precision, recall, and F1-score compared to the other methods. The ANOVA test was performed to validate these differences.

From the Table 9 the ANOVA results indicate a significant difference between the methods, with the proposed model showing superior performance.

From the Table 10 the proposed model shows lower MAE, RMSE, and MAPE values, indicating better performance in predicting disease progression. The ANOVA test validates these results.

From the Table 11 the ANOVA results confirm the statistical significance of the differences observed in the prediction performance.

Table 12. Anomaly detection performance

Method	True Positive Rate (%)	False Positive Rate (%)	Precision (%)	F1-Score (%)
Proposed	94.5	3.2	93.8	94.1
Method [3]	89.0	5.8	88.0	88.5
Method [8]	86.3	7.0	85.0	85.6
Method [14]	87.5	6.5	86.0	86.7

Table 13. ANOVA results for anomaly detection

Source of Variation	SS	df	MS	F	P Value
Between Groups	106.7	3	35.57	22.48	0.0003
Within Groups	25.3	16	1.58		
Total	132.0	19			

Table 14. Data security and integrity

Method	Data Tampering Incidents	Unauthorized Access Attempts	Data Integrity Score (%)
Proposed	0	0	100
Method [3]	1	1	98
Method [8]	2	2	96
Method [14]	1	1	97

Table 15. ANOVA results for data security and integrity

Source of Variation	SS	df	MS	F	P Value
Between Groups	0.0063	3	0.00210	14.50	0.0005
Within Groups	0.0023	16	0.00014		
Total	0.0086	19			

Table 16 Privacy preservation metrics

Method	Privacy Loss (ϵ\epsilonϵ)	Utility Loss (%)	Accuracy of Private Results (%)
Proposed	0.7	3.0	97.0
Method [3]	1.1	4.8	95.2
Method [8]	1.4	6.3	93.7
Method [14]	0.9	4.0	96.0

Table 17. ANOVA results for privacy preservation metrics

Source of Variation	SS	df	MS	F	P Value
Between Groups	0.0087	3	0.00290	16.75	0.0004
Within Groups	0.0028	16	0.00018		
Total	0.0115	19			

The proposed model achieves a higher true positive rate and a lower false positive rate. ANOVA results validate these differences.

From the Table 12 the ANOVA test shows a significant difference in anomaly detection performance among the methods.

From the Table 13 the proposed model ensures higher data security and integrity. The statistical validation using ANOVA confirms these observations.

From the Table 14 the ANOVA results validate the statistical significance of the security and integrity measures.

From the Table 15 the proposed model exhibits superior privacy preservation with lower privacy loss and utility loss, while maintaining high accuracy of private results. ANOVA tests confirm these findings.

From Table 16 and Table 17 there are significant differences in the metrics preserving privacy among algorithms, as indicated by the ANOVA test. ANOVA tests for statistical validation in support of the proposed Smart Healthcare System with regard to performance metrics confirm the model's superiority. The model accuracy pertaining to disease occurrence is 90.2%, much higher than comparative methods [3, 8, 14], validated by an F Value of 23.76 and a p Value of 0.0001. There is a lower MAE, RMSE, and MAPE for the prediction of disease progression by the LSTM network. Differences were significant with an F Value of 18.04 and p Value of 0.0002. It showed that the proposed model was much better in terms of anomaly detection performance measured with a true positive rate of 94.5% and a false positive rate of 3.2%. Independent examples are validated with an ANOVA F Value of 22.48 and a p Value of 0.0003. The results on data security and integrity show that the Ethereum Blockchain implementation is very robust, with no data tampering incidents, while it emerged perfect in data integrity, confirmed by an ANOVA F Value of 14.50 and a p Value of 0.0005. The privacy preserving metrics are such that through this proposed model, it ensures ϵ=0.7, and at this privacy budget, the loss incurred in utility is only about 3.0%. Moreover, the accuracy of the private results is maintained at 97.0%. Results are statistically significant with ANOVA's F Value of 16.75 and a p-value of 0.0004. This proposed model ensures much more accuracy, anomaly detection, data security, and preservation of privacy as compared to major characterised methods, which were asserted by rigorous statistical analysis. This is a full-fledged assessment of the potential discussed by this proposed Smart Healthcare System with regard to revolutionizing the healthcare sector in both patient care and data management.

5. CONCLUSION AND FUTURE SCOPES

For medical data analysis and patient care, IoT and AI in Smart Healthcare System development have been growing manifoldly. In the present research, a comprehensive model design has been proposed that integrates hybrid machine learning models, long short-term memory networks, Ethereum blockchain with smart contracts, and homomorphic encryption along with differential privacy techniques. Experimental

results prove that the proposed model is efficient and effective in improving the accuracy of disease prediction, the tracking of diseases, securing the patient's data, and maintaining privacy. In this paper, the implemented Hybrid ML model confers an excellent accuracy for disease prediction using a random forest classifier with k-means clustering of about 89.5%, as compared to the previously published methods [3, 8, 14] with accuracies of 85.2%, 80.7%, and 82.3%, respectively. The precision and recall metrics, 88.0% and 90.5%, respectively, further suggest that it is quite wholesome in the identification of high-risk patient groups, not providing disease occurrence probabilities that are reliable but also capable of predicting disease development and anomaly detection. For instance, the mean absolute error was 0.045, and the root mean squared error was 0.065 for the LSTM network in the prediction of disease progression and anomaly detection. These metrics put the model at high precision in timestamp series analysis, above comparative methods reporting higher error rates. The true positive rate for the detection of anomalies was 93.0%, while the false positive rate was very low at 3.5%, which signifies high sensitivity and specificity for the model to pick out anomalous health events.

Data security and integrity were guaranteed by the implementation of Ethereum Blockchain with Smart Contracts, giving no chances to data tampering incidents or unauthorized access attempts. The obtained data integrity score using the proposed model was 100%, while that for the other methods stood at 98, 96, and 97%. This robust security framework is therefore of paramount importance for protecting patients' trust and for compliance with the strictest regulations related to personal data protection, such as GDPR. With a view to ensuring privacy preservation and guaranteeing utility, homomorphic encryption and differential privacy methods were very effectively balanced. The inoculated privacy loss value was $\epsilon = 0.8$, while the utility loss incurred was only 3.5%. These ensure that private results remain very accurate at 96.5%. It is quite clear from the results that a model performing privacy-preserving computations without huge losses in data utility is very feasible. The overall performance of the proposed model was beyond existing methods in all metrics evaluated, thus having the potential to revolutionize smart healthcare systems. In that respect, it not only integrates advanced machine learning techniques and secure blockchain technology but also privacy-preserving methods to provide an all-rounded solution against the complex challenges of modern healthcare.

Since the model has to be based on clinical decisions, it is rather important that it be interpretable; medical practitioners need to understand what exactly contributes to any prediction, especially in high-risk patients. So, inside this model, feature importance from Random Forest and Local Interpretable Model-agnostic Explanations (LIME) is used to interpret the predictions such that clinicians may understand which features contribute the most to each risk score for a given patient. For instance, the Random Forest classifier calculates the feature importance based on Gini impurity reduction which, in turn, focuses on the key health indicators like blood pressure, age, cholesterol levels, smoking, and so on or the process. This enables the model to provide results explainable through how much contribution every feature is toward making a high-risk prediction, measurable and visualized in process. The model will then, for example, indicate the contribution of components-for example, high blood pressure at 30%, high cholesterol levels at 25%, and smoking status at 20%--to the risk assessment that is mostly predictive of the outcomes. SHAP values also give a patient-specific view of how each feature impacts the prediction outcome. SHAP assigns an influence value to each feature and aids clinicians in getting to know the exact factors that contribute to a warning in a particular case. For example, SHAP values in the case of a high-risk prediction for cardiovascular diseases would indicate that recent increases in blood pressure and abnormal heartbeat recordings are the main risk factors. Interpretability techniques not only predict whom are likely at risk but also allow the model to be transparent about how it is making decisions so that their health care provider can communicate specifically what those risk factors are for the patients and potentially make the process much more informed, data-driven decisions. These interpretability tools are useful in building a bridge between complex model predictions and practical medical use, thereby making the model more trustworthy and useful for use in clinical settings.

5.1 Future scope

The results from this research open various avenues of future research and development in the domains of smart healthcare systems. Otherwise, scalable architectures with real-time processing and execution capabilities can make this model even more responsive in different health settings. This paper makes use of edge-based computing for its scalability and cloud-based services to handle large-scale data that helps provide instant health monitoring and prediction. Enhancement of the model supporting approaches to personalized medicine by admitting genetic data, design of personalized treatment plans, and patient-specific risk factors creates a more accurate health care intervention tailored to each patient outcome. Added data sources such as genomic data, wearable devices, and social determinants of health help create a fuller dataset to establish a holistic view of a patient's health. Interoperability and standardization of data formats and protocols to ensure seamless integration with existing healthcare systems and electronic health records. This can enhance data sharing, collaboration, and the take-up of smart healthcare technologies. Address ethical and legal issues related to data privacy, consent, and patient rights. Develop frameworks and guidelines that should ensure that the implementation of smart healthcare systems is made in such a way that justifiable ethical values are followed and appropriate regulations complied with accordingly. It is the research in these lines that can be taken ahead in the future and can add to the foundation laid by this research in its effort to continuously evolve smart healthcare systems for their effect on scenarios of patient care and public health scenarios.

REFERENCES

[1] Pradhan, B., Das, S., Roy, D.S., Routray, S., Benedetto, F., Jhaveri, R.H. (2023). An AI-assisted smart healthcare system using 5G communication. IEEE Access, 11: 108339-108355. https://doi.org/10.1109/ACCESS.2023.3317174

[2] Zhou, B., Yang, G., Shi, Z., Ma, S. (2022). Natural language processing for smart healthcare. IEEE Reviews in Biomedical Engineering, 17: 4-18. https://doi.org/10.1109/RBME.2022.3210270

[3] Alruwaili, F.F., Alabduallah, B., Alqahtani, H., Salama,

A.S., Mohammed, G.P., Alneil, A.A. (2023). Blockchain enabled smart healthcare system using jellyfish search optimization with dual-pathway deep convolutional neural network. IEEE Access, 11: 87583-87591. https://doi.org/10.1109/ACCESS.2023.3304269

[4] Akter, M., Moustafa, N., Lynar, T., Razzak, I. (2022). Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. IEEE Journal of Biomedical and Health Informatics, 26(12): 5805-5816. https://doi.org/10.1109/JBHI.2022.3192648

[5] Saini, A., Wijaya, D., Kaur, N., Xiang, Y., Gao, L. (2022). Lsp: Lightweight smart-contract-based transaction prioritization scheme for smart healthcare. IEEE Internet of Things Journal, 9(15): 14005-14017. https://doi.org/10.1109/JIOT.2022.3145406

[6] Thapliyal, S., Wazid, M., Singh, D.P., Das, A.K., Shetty, S., Alqahtani, A. (2023). Design of robust blockchain-envisioned authenticated key management mechanism for smart healthcare applications. IEEE Access, 11: 93032-93047, https://doi.org/10.1109/ACCESS.2023.3310264

[7] Raina, R., Jha, R.K. (2022). Intelligent and interactive healthcare system (I 2 HS) using machine learning. IEEE Access, 10: 116402-116424. https://doi.org/10.1109/ACCESS.2022.3197878

[8] Syu, J.H., Lin, J.C.W., Srivastava, G., Yu, K. (2023). A comprehensive survey on artificial intelligence empowered edge computing on consumer electronics. IEEE Transactions on Consumer Electronics, 69(4): 1023-1034. https://doi.org/10.1109/TCE.2023.3318150

[9] Wu, G., Wang, S., Ning, Z., Zhu, B. (2021). Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system. IEEE Journal of Biomedical and Health Informatics, 26(5): 1917-1927. https://doi.org/10.1109/JBHI.2021.3123643

[10] Islam, M.M., Bhuiyan, Z.A. (2023). An integrated scalable framework for cloud and IoT based green healthcare system. IEEE Access, 11: 22266-22282. https://doi.org/10.1109/ACCESS.2023.3250849

[11] Mallick, S.R., Lenka, R.K., Goswami, V., Sharma, S., Dalai, A.K., Das, H., Barik, R.K. (2023). BCGEO: Blockchain-assisted geospatial web service for smart healthcare system. IEEE Access, 11: 58610-58623. https://doi.org/10.1109/ACCESS.2023.3283776

[12] Ali, M., Naeem, F., Tariq, M., Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. IEEE Journal of Biomedical and Health Informatics, 27(2): 778-789. https://doi.org/10.1109/JBHI.2022.3181823

[13] Wazid, M., Das, A.K., Shetty, S. (2022). BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare. IEEE Transactions on Consumer Electronics, 69(1): 18-28. https://doi.org/10.1109/TCE.2022.3208795

[14] Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q., Shen, X. (2021). A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics, 18(3): 2021-2031, https://doi.org/10.1109/TII.2021.3098010

[15] Abdeen, M.A., Ahmed, M.H., Seliem, H., Sheltami, T.R., Alghamdi, T.M. (2022). Smart health systems components, challenges, and opportunities. IEEE Canadian Journal of Electrical and Computer Engineering, 45(4): 436-441. https://doi.org/10.1109/ICJECE.2022.3220700

[16] Egala, B.S., Pradhan, A.K., Dey, P., Badarla, V., Mohanty, S.P. (2023). Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system. IEEE Internet of Things Journal, 10(14): 12308-12321. https://doi.org/10.1109/JIOT.2023.3247452

[17] Almas, A., Iqbal, W., Altaf, A., Saleem, K., Mussiraliyeva, S., Iqbal, M.W. (2023). Context-based adaptive fog computing trust solution for time-critical smart healthcare systems. IEEE Internet of Things Journal, 10(12): 10575-10586. https://doi.org/10.1109/JIOT.2023.3242126

[18] Gao, J., Nguyen, T.N., Manogaran, G., Chaudhary, A., Wang, G.G. (2022). Redemptive resource sharing and allocation scheme for Internet of Things-assisted smart healthcare systems. IEEE Journal of Biomedical and Health Informatics, 26(8): 4238-4247. https://doi.org/10.1109/JBHI.2022.3169961

[19] Li, J., Li, D., Zhang, X. (2023). A secure blockchain-assisted access control scheme for smart healthcare system in fog computing. IEEE Internet of Things Journal, 10(18): 15980-15989. https://doi.org/10.1109/JIOT.2023.3268278

[20] Hajjej, F., Javeed, M., Ksibi, A., Alarfaj, M., Alnowaiser, K., Jalal, A., Alsufyani, N., Shorfuzzaman, M., Park, J. (2022). Deep human motion detection and multi-features analysis for smart healthcare learning tools. IEEE Access, 10: 116527-116539. https://doi.org/10.1109/ACCESS.2022.3214986

[21] Bao, Y., Qiu, W., Cheng, X. (2021). Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system. IEEE Internet of Things Journal, 9(4): 2513-2526. https://doi.org/10.1109/JIOT.2021.3063846

[22] Lin, Y.H., Tang, H.S., Shen, T.Y., Hsia, C.H. (2022). A smart home energy management system utilizing neurocomputing-based time-series load modeling and forecasting facilitated by energy decomposition for smart home automation. IEEE Access, 10: 116747-116765. https://doi.org/10.1109/ACCESS.2022.3219068

[23] Rana, B., Singh, Y., Singh, P.K., Hong, W.C. (2024). A priority based energy-efficient metaheuristic routing approach for smart healthcare system (SHS). IEEE Access, 12: 85694-85708, https://doi.org/10.1109/ACCESS.2024.3411564

[24] Islam, M.M., Nooruddin, S., Karray, F., Muhammad, G. (2022). Internet of things: Device capabilities, architectures, protocols, and smart applications in healthcare domain. IEEE Internet of Things Journal, 10(4): 3611-3641. https://doi.org/10.1109/JIOT.2022.3228795

[25] Fan, J., Yang, W., Liu, Z., Kang, J., Niyato, D., Lam, K.Y., Du, H. (2023). Understanding security in smart city domains from the ANT-centric perspective. IEEE Internet of Things Journal, 10(13): 11199-11223. https://doi.org/10.1109/JIOT.2023.3252040