International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

Hybrid Classification Model for Patient Data Detection using Encryption and Decryption in Cloud Environments

Ruth Athertan*

University College London, London, UK

Received 20 Jan 2025, Accepted 08 Feb 2025, Available online 10 Feb 2025, **Vol.13 (Jan/Feb 2025 issue)**

Abstract

Cloud computing has redesigned the healthcare industry through the means of secure and efficient data management and the timely processing of patient information. However, with the absolute ever-increasing healthcare data, protecting sensitive information during storage and transmission has remained a big challenge. In this paper, a hybrid classification model is proposed: the mechanism integrates well-established encryption techniques, such as RSA for encryption and AES for decryption, with contemporary machine learning methods like CNN (Convolutional Neural Networks) and Autoencoders for data classification. It aims at ensuring the confidentiality and integrity of healthcare data within the cloud space along with a highly accurate and efficient classification of health conditions. The hybrid model hence aims at enhancing the anomalous detection capacity along with thus securing highly cloud-based healthcare systems from data breaches and unauthorized access. Evaluation results have shown that the proposed system is very accurate and reliable, which promotes its potential as a suitable solution for securing healthcare data management.

Keywords: *Cloud Computing, Health Care, Healthcare Data Security, Machine Learning, Healthcare Data Management*

1. Introduction

Cloud computing has certainly made huge strides for healthcare by permitting the management, storage, and even real-time analysis of data. Being able to store and analyze large amounts of data in remote cloud-setting environments has created several transformative changes relating to availability, efficiency, and collaboration among healthcare systems [1]. The sharing of patient data instantly, including electronic health records (EHRs), medical images, diagnostic results, and other relevant health data, helps healthcare professionals make better decisions and provide even better patient care and faster health outcomes[2]. Installation among the different medical systems can also be achieved through a cloud infrastructure, letting one analyze real-time data and study changes in response to new information about patient progress.

However, as more cloud systems are used for patient information management, these concerns about security and privacy have come to the fore front. The transfer, safekeeping and operations on large quantities of sensitive data through the internet vulnerates healthcare systems from various cyber-security issues including data breaches, intrusion, cyber-attacks. These concerns are escalated by the growing amount of healthcare data that is now being transferred between institutions such as medical records, test results, diagnostic imaging that needs to be passed on to different platforms and entities for efficient collaboration. Moreover, the fast development of Internet of Things (IoT) devices, which are critically important in real-time patient tracking, increases the attack surface many-fold, thus making the management of security even more challenging. It is therefore essential to ensure that the confidentiality, integrity and the availability of patient data is ensured since any failure on this front can result in dire consequences in terms of patient safety and confidence [3]. By combining AI, middleware, and blockchain for secure healthcare data exchange, Winner Pulakhandam et al.'s (2024) [4] work has guided the proposed system towards enhancing the security and efficiency of healthcare data classification in cloud environments.

With these shifting security threats, there is even more need for the need of strong encryption mechanisms which can protect healthcare data while being transmitted and stored [5]. Traditional forms of encryption such as RSA and AES are usually employed to secure sensitive information but it often comes at the expense of performance and it is particularly critical in real-time systems where a low latency is required. This

*Correspondant Author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr/v.13.1.5

issue becomes especially timely when the amounts of large-scale healthcare data are discussed because the computational burden of such encryption and decryption undertakings may slow down decision-making and compromise the urgency of medical procedures. This has thus led to the need for improved encryption techniques in the healthcare systems, which should be efficient, but not significantly harm the performance. Additionally, with the constant development of cyber threats, there is an urgent need for the adaptive systems that are able to defend against the new forms of attacks while ensuring the integrity of patient data [6].

The dependence on cloud computing also requires the adoption of sophisticated machine learning methods not only to secure the data but to also enhance the analysis of healthcare data [7]. Machine learning algorithms, especially for anomaly identification, and classification, can assist in real-time identification of security threats, like unauthorized access or data breach. With the help of large datasets, training these algorithms in the healthcare systems can make them more proactive in the detection of suspicious activity and prevention of such breaches beforehand. In addition to this, these algorithms can also be used for predictive health analytics so that healthcare providers can spot patterns or trends that can suggest some emerging conditions. Integration of modern machine learning models with cloud-based security schemes can thus optimize the security of healthcare systems, as well as their efficiency, improving patients' outcomes and ensuring strict data privacy. As Gudivaka (2024) [8] has shown, the incorporation of AI-driven healthcare solutions for health monitoring has had a significant impact on the proposed work in improving the security and accuracy of healthcare data classification in cloud environments.

Managing healthcare data in cloud settings is complex because of the need to find a balance between the elasticity, and scalability, and rigorous security needs [9]. Healthcare data has to be protected from manipulation or loss, in addition to their inaccessibility to unauthorized users, while capabilities of the system developing are also preserved [10]. Some of the traditional methods of securing data such as encryption and decryption are usually used to protect sensitive information. however, these mechanisms can add computational overhead, especially in a real-time system where fast decision is needed. This backlog in processing can create a bottle-neck on the rate at which healthcare providers may respond to critical patients' needs. Besides, traditional security procedures may be unable to cope with the fast-changing cyber threats environment, and there was a need to create advanced security solutions [11].

This problem can be addressed by using a hybrid method for classification that increases security and the accuracy of classification by combining encryption techniques with sophisticated machine-learning algorithms. That is, encryption and decryption techniques protect the patient data from access, whereas doctors can open the data in a secure environment to classify and detect anomalies. The machine learning models of Random Forest and Support Vector Machines (SVM) can aid the system in processing and classification of data to recognize any pattern that may be suggestive of a potential health condition or anomaly. The use of hybrid classification also evidences an enhancement in the capability of identifying complex patterns from healthcare-related data for prediction, which diminish the chances of illegal access.

The proposed hybrid model not only strengthens security measures and strengthens the privacy of healthcare data but also optimizes the efficiency of cloud-based healthcare systems. By incorporating best-of-breed encryption systems with powerful machine learning algorithms, the approach enhances health condition detection accuracy and thus allows healthcare systems to care better for patients while protecting sensitive data. Integrating the model with clinical patient record systems can return considerable benefits in reliability, scalability, and security of the cloud databases, which ensure that healthcare delivery becomes safer and efficient. The model can further be tailored for use throughout various healthcare establishments, encouraging collaboration while improving healthcare outcomes on a larger scale.

1.2 Problem Statement

The actual hybrid classification model builds upon the back of secure and efficient encryption methods, such as RSA and AES encryption for transmission and decryption, combined with CNN and an Autoencoder in machine learning (ML), allowing for the secure handling of private healthcare data. It ensures very high security through encryption of a patient's information during transmission and information processed securely on cloud systems, but this very combination also instances work on the optimization of encryption and decryption that worth every consideration that assumes a real-time application model. The hybrid classification model further improves both the anomaly detection and classification accuracy, which, as a result, provides high security for cloud health systems while dealing with the advanced threat of attacks.

1.3 Objectives

Cloud computing issue has pervaded every aspect of our daily lives, like in healthcare, by allowing secure and efficient management of data with real-time analysis of patient information. However, as healthcare data grows exponentially, it still remains a primary challenge to provide security to sensitive information during storage and transmission. This paper proposed a hybrid classification model that is based on strong encryption methods including RSA for encryption and AES for decryption, on the one hand, and advanced ML techniques such as CNN and Autoencoders for data

classification, on the other. Our approach provides confidentiality and integrity to the healthcare data hid in a cloud environment and allows classifying the health conditions in an accurate and efficient manner. The hybrid model enhances the anomaly detection capabilities while also ensuring good security in cloud-based health care systems, thus reducing the chances of unauthorized access and data breaches. Evaluation results show that our solution provides a high level of accuracy and reliability hence is a good solution for secure healthcare data management and analysis.

2. Literature Survey

The finance and e-commerce sectors are more and more popularizing the use of cloud computing, smart networks, and blockchain to attain enhanced scalability, security, and efficiency in the massive data environment. On-the-go technology acts towards resource management enhancement, secure transactions, and system scalability upgrading. Cloud-based resource management combined with IoT-driven analytics and blockchain will enhance enterprise operational efficiency and transaction security. Selected real-case studies have aforementioned that this integration positively turbans performance in the perspective of e-commerce and finance systems. Cloud computing, artificial intelligence, and the IoT have changed healthcare with real-time monitoring and diagnosis. The combination of IoT with cloud computing platforms, as well as hybrid neural-fuzzy learning models, augments the accuracy of diagnostics and assists in decision-making. By combining machine learning and fuzzy logic, this system effectively handles huge amounts of medical data either to predict normal or abnormal health conditions. It also assures scalability, dependability, and real-time monitoring of patients.

Lung cancer, with adherence to the classification of either small cell or non-small cell types, nevertheless continues to challenge global health. It is the application of graph theory that recently emerged in this realm to depict the complex molecular interactions involving genes and proteins as interlaced nodes. This gives the methodologies the potential to identify biomarkers and predict the course of the diseases, in addition to aiding in the choice of drug targets for treatment. Machine learning, on the other hand, allows for even more refined precision in recognizing and predicting lung cancers. The inclusion of CDN and hybrid cloud solutions to enhance mobile multimedia health record management, as developed by Venkata Sivakumar Musam et al. (2024) [12], inspired the proposed framework for secure healthcare data classification and retrieval.

Much data is being produced in the healthcare sector at a furious speed, which is the basis for accurate assessment and decision-making by sophisticated analytics methods. The cloud-based inference ecosystem integrates a series of machine-learning models aiming toward the analyses of complex healthcare datasets, increasing interpretability and scalability [13]. Treating the problems of sparsity and algorithmic transparency, the framework offers meaningful insights that aid in the clinical decisions of health practitioners. The ensemble method enhances predictive potential, making the lives of practitioners easy, and providing for great patient care and resource utilization. Cloud computing has revolutionized the possible management of it as an integrated utilization of scalable storage, applications, and processing power. The current research investigates resource allocation optimization in cloud data centres by advanced load balancing strategies. This works well with edge computing, AI, and machine learning to create an improved scalable, efficient, and effective performance of the system [14]. Intelligent distribution of workloads can improve efficiency in resource usage and responsiveness in a dynamic cloud environment.

More and more the mobile internet access is growing in Africa, and this has penetrated even connectivity in rural areas, where, however, financial inclusion is lacking in e-commerce. The study, therefore, looks into internet-inclusive finance for rural connectivity and its importance to entrepreneurship and business growth in rural areas. Data-driven analysis as a finding shows that income levels and economic opportunities yield positive effects. This will in increasing internet access and financial inclusion greatly contribute towards reducing the urban-rural gap for socioeconomic progress. With the help of Cloud IoT and digital financial inclusion, underserved communities can access financial services, which significantly reduces income inequality. This paper focuses on defining how income gaps between urban and rural areas have been bridged and how it creates economic equity and poverty alleviation. In advanced analyses, Cloud IoT-driven financial inclusion improved the distribution of income than traditional financial inclusion avenues [15]. It states that lending sustainable digital financial access serves an equalizing development and equitable financial policy in the economy.

Digital finance, with a cloud foundation, helps to realize financial inclusion by removing traditional hindrance features and by bridging urban versus rural income gaps. The consequences for access to transaction costs, financial services, and economic equality. The results suggest a significant improvement in terms of financial inclusion for the rural communities by cloud technology that enhanced accessibility and savings opportunities. Further, the support of cloud technology to digital finance floats a platform for inclusive economic development through narrowing financial gaps. This design serves equal access to finance, therefore promoting sustainable development. With the advance in cloud computing, securing data is an important necessity for preventing various threats like theft and manipulation. A quadruple layer of security integrating cryptography with LSB steganography in order to confer maximum protection. Confidential data is embedded into the pixels of images, while encryption keys are secured by AES and

RSA, thereby providing a fine layer of protection to confidentiality and integrity over cloud environments. It works on the major challenges concerning embedding efficiency, security vulnerabilities, and computational complexity.

Having prepared fog computing systems to enhance their performance and reduce latency, data sharing and resource allocation security for IoT environments still remain a challenge to be worked on. The present paper proposes a hybrid clustering model of fuzzy C-Means, DBSCAN, and ABC-DE optimization to improve the efficiency and accuracy of fog computing. The approach provides enhanced secure data flow in the mist while optimizing bandwidth and ensuring the operation of reliable IoT-fog systems. The results indicate superior performance in security, resource allocation, and scalability compared with traditional methods. The combination of IoT and Big Data Analytics into Business Intelligence systems, as shown by Priyadarshini Radhakrishnan et al., (2024) [16] plays a key role in developing the proposed research by guiding the development of secure healthcare data processing models using advanced analytics.

Tunnel engineering involves significant risks, long construction timelines, and high costs. Tunnel Boring Machines (TBMs) play a vital role in improving efficiency and safety by collecting vast amounts of monitoring data. To enhance safety management and decision-making, A hybrid data mining approach for automating the real-time processing of TBM data. By integrating association rule mining, decision tree classification, and neural network models, the system analyses TBM parameters, detects anomalies, categorizes geological formations, and predicts the rate of penetration (ROP). Applied to a tunnel project in China, this method significantly boosted operational efficiency and safety management by analysing TBM data with high precision and effectiveness.
A timely diagnosis is necessary for effective intervention for neurological disorders, but most traditional methods fail in sensitivity [17]. An AI model that integrates PSP Net for high-level feature extraction, Hilbert-Huang Transform (HHT) for complex signal analysis, and fuzzy logic for data uncertainty handling. The system enhances diagnostic accuracy by analysing brain signals and discriminating between different neurological disorders. Equipped with a graphical user interface, the model is aptly designed for clinical settings, attaining an accuracy of 95%, compared to traditional methods. Combining PSP Net, HHT, and fuzzy logic within this system improves early detection, a huge step forward with regard to precision diagnosis in neurological disorders [18].

For purposes of preventing cardiovascular disease (CVD) in patients with rheumatoid arthritis (RA), an accurate risk prediction model becomes crucial [19]. The stability of those biomarkers over 10-to-20-year-old periods, including lipid profiles and inflammatory markers. Risk prediction models are developed for RA populations by integrating classical risk factors with RA-specific ones such as disease activity. The advanced technologies-facilities including wearables and telemedicine platforms-and omics data are being incorporated into cardiovascular risk assessment and patient monitoring. The main goal of this study will include improving cardiovascular risk prediction through longitudinal data analysis and clinical translation to inform individual therapy and a further enhance patient outcome in RA populations.

Cloud computing-based data storage solutions are scalable and comparatively less expensive and thus have transformed several industries. However, the healthcare industry, with its extremely sensitive patient data and stringent regulatory norms, suffers the most from security challenges. A comprehensive security management system is presented to meet these challenges that comprise risk analysis, security implementation, continuous monitoring, and compliance management. Through risk assessments, the security management system identifies potential threats and implements various security measures such as encryption, authentication, and intrusion detection. It uses the most modern technology, like multi-factor authentication and blockchain, to further enhance the security posture. The case studies of the Cleveland Clinic and Mayo Clinic represent the successful use of cloud computing while maintaining data security, which ultimately benefited patient care and operational efficiency.

In the contemporary cyber-attack landscape with swiftly changing threats and ever-sophisticated attacks, cybersecurity risk management is essential. Previous research in this area has, however, focused more on assessment and management of risks without much intelligence into threat properties and changes in attack trends, resulting in credible but limited contextual data for the relevance of cybersecurity risks. The Merged Cyber Security Risk Management method (m-CSRM) that addresses these challenges by identifying critical assets utilizing a decision support system based on fuzzy set mechanisms. Furthermore, it predicts risk types through machine learning algorithms processed using an automated tool. The proposed method of m-CSRM gives an outcome of 82.13% and hence stands next to all the old methods for efficiency and effectiveness. The integration of CNN-LSTM and Neuro-Fuzzy for CKD prediction, as explained by Alagarsundaram et al. (2024) [20], enthused the proposed approach to incorporate machine learning and encryption for secure healthcare data classification.

An innovative approach to enhancing workload forecasting in intelligent cloud computing systems that include a Backpropagation neural network algorithm and game theory principles [21]. The methodology is designed to strategically align the interests of cloud users and service providers so that resources can be optimally allocated or serviced. Using concepts of the Nash equilibrium, this study aims to accomplish win-win situations by establishing Service Level Agreements (SLAs)

for all stakeholders. The experimental validation on real-world data demonstrates how this approach improves operational efficiencies in cloud computing towards strategic alignment [22]. The proposed method focuses on scalability, security, and usability and has great potential for cloud resource management improvements in various industries.

Attacks and protection of data privacy assume an important role in collaborative computing systems, which represent significant issues in this research [23]. The latest technologies such as federated learning and cloud-edge collaborative computing systems to create multi-national validation architecture under attack and non-attack scenarios. Via the privacy-preserving way of classifying attacks, End-to-end privacy-preserving deep learning (E2EPPDL) becomes another crucial aspect of this study. The research is validated using important metrics Routing Count, Time, Node Count, and Data Delivery Ratio; proving the proposed approach to be efficient regarding security and privacy within collaborative computing systems.

Transformation of modern industry IoT from all angles, especially enterprise information management and optimization of the supply chain, is providing an important part for the manufacturing industry. However, introducing IoT features into a manufacturing system brings various challenges for inventory cost control and job-shop scheduling (JSP), where the main task is to optimize production in extremely difficult and dynamic constraints. A new approach for JSP solution, using Hybrid Particle Swarm Optimization (HPSO) and Heterogeneous Genetic Algorithm (HGA). In HGA, an immune mechanism, including memory and mutation strategies, is incorporated into a traditional Genetic Algorithm (GA) to avoid the early convergence and enhancement of exploration capabilities. HPSO is proposed to advance job sequencing for minimizing production time. Thus, this hybridization allows HPSOs to equalise global and local search efficiency, preparing HPSOs more effectual than out-dated PSOs in handling intricacies in JSP. In addition to this, it will also enhance the cost optimization and scheduling performance of HPSOs. Furthermore, huge contributions were made within the field through hybridizing genetic algorithms with HPSO and doubles of chain-encoded machine selection and job sequencing. The method was validated using empirical study, and it shows that HGA and especially HPSO can outstrip out-dated scheduling methods. The development of an efficient healthcare data classification model in the proposed technique is shaped by the use of B-Cloud-Tree indexing for cloud service selection, enhancing retrieval speed and accuracy, as exemplified by Yalla, R. K. M. K. (2021) [24].

An improved heart disease monitoring scheme that applies IoMT devices associated with the technology blockchain for accurate prediction inputs of heart diseases including arrhythmias and ECG and PCG signals [25]. The system has been designed to securely register both doctor and patient, generates cryptographic keys, and uploads the sensed data files to IPFS. The data gets secured in a hash code that is stored in the blockchain and authenticated through MAC verification. The classified heart diseases in the system undergo preprocessing where data is processed through signal decomposition and feature extraction for prediction on heart diseases [26]. The proposed OA-CNN method scored a high accuracy of 98.32% and won over other models, proving to be a better solution in heart disease detection.

A state-of-the-art novel strategy for educational governance through an intelligent education management platform utilizing cloud computing blended with artificial intelligence (AI) [27]. The development enhances educational services through intelligent automation and personalized learning by leveraging the capabilities of AI while cloud computing gives a scalable and efficient way of data management. SOA is the architectural design on which this system was built, which was implemented in a Hadoop-managed server cluster. This kind of cloud application will support large data access, as well as high concurrency, which make very smooth remote learning and efficient resource management possible. Stress tests indicate that the platform can handle heavy loads that invariably demand capacity for multiple users and many data transactions but without compromise in reliability. AI-based features such as recommendation engines and predictive analytics significantly redefine overall learning experiences, giving a glimpse into how this platform can improve education in terms of service delivery.

3. Methodologies

The process of secure healthcare data classification is demonstrated in Figure 1 through a complete flow. At first, a patch collects patient data (EHR, medical images, sensor data), etc. To keep this raw data confidential during transmission encryption process has to be applied and this is done using the RSA algorithm. The RSA encryption makes sure that the data is safe even when it is transmitted through the potentially compromised networks and so the patient information is kept secure. When the encrypted data comes to the cloud server, it is decrypted with the help of the AES (Advanced Encryption Standard) algorithm. AES is a symmetric method of encryption that allows to decrypt the encrypted data to get it back to a normal state for further processing and analysis in a safe environment. Once decrypted, the data gets preprocessing, whereby, it is cleaned, normalized, and missing values are dealt with. This preprocessing guarantees that the data is put in an appropriate state for analysis through the removal of irrelevant or noisy data. The preprocessed data is then put over a hybrid CNN and Autoencoder model. CNN part extracts significant spatial features from medical images or sensor data, while Autoencoder ensures the dimensionality reduction and

elimination of unnecessary features thus allowing the classification process to be more effective. The step of classification determines whether a person has a health condition or not. If a condition occurs, the data is being tagged 'Detected', otherwise it is tagged as 'Not Detected'. The final ones (but not the least important), the performance of the model is assessed with effective metrics of accuracy, precision, and recall which facilitate calculating the effectiveness of the procedure of classification of health conditions. Such metrics provide essential feedback, for further enhancement of the model to enhance better and reliable classification of data for healthcare purposes.

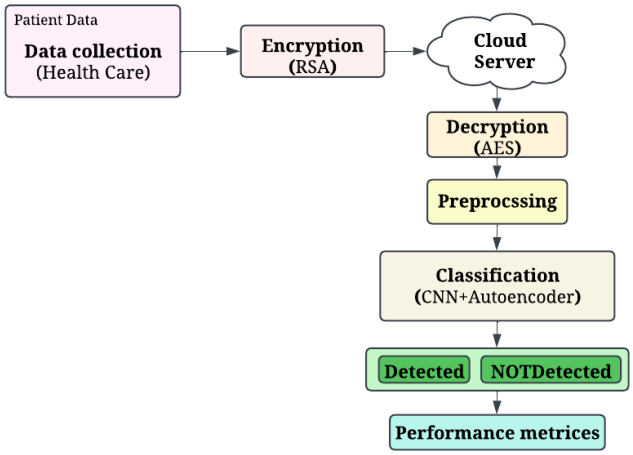

Figure 1: Secure Healthcare Data Classification in Cloud

3.1 Data Collection

Healthcare has to process a variety of patient data, including patients' EHRs, medical images as well as data from such sensors embedded in devices such as monitors of patients' heart rate and ECG. The EHRs provide the full picture of the medical treatment history with a patient. Medical images are useful to visualize the disorders in them; and sensor data is useful to monitor the vital parameters which are associated with the patient on a real-time basis. Therefore, it is extremely crucial to make data correct, complete and standardized as these parameters would directly affect the operation of predictive models. There are a number of barriers that have to be overcome, including privacy of the data, missing data, and cross-platform integration. Preprocessing, labelling, and integration of data thus forms a good healthcare detection system.

3.2 Encryption

Patient information in this case is securely encrypted thus making it confidential regardless of chances of insecurity of the computer networks that it is transmitted over. There are asymmetric encryption algorithms that are used to encrypt sensitive information, for instance, health records, medical images, and other patient material, and RSA (Ronald Rivest, Adi Shamir, and Len Adelman) which is one of such algorithms is used to prevent the transfer of the said information to unauthorized people. Prior forwarding the patient data to the cloud server, message M (the plaintext data) is first transformed to m by mapping each character of the message to the integer. This change is essential, as RSA encryption works with numbers and not with textual data. By improving BCI systems with Transfer Learning and Edge AI, as shown by Budda (2021) [28], the proposed research incorporates similar AI-driven models to optimize healthcare data classification, ensuring efficient processing and security.

The encryption process starts by taking the original message M and converting it into an integer m, such that m is less than the modulus n (i.e., $m < n$). The next step involves applying the RSA encryption algorithm to transform the integer m into ciphertext c, which is unreadable without the corresponding private key. This transformation is carried out by the equation;

$$c = m^e \bmod n \qquad (1)$$

In this equation, c is called ciphertext, the encrypted version of the message. m is the numeral form of plaintext message m^e is the public exponent, which is part of public key, and it is used in the encryption process. n is called modulus, which is a large number obtained as the product of two prime numbers during the key generation process.

The encryption operation consists in raising integer m to a power e and then returning the result modulo n [29]. This guarantees that the enciphered data c can only be decrypted through the private key that has no superior form of relationship with the public key but the mathematical relationship that makes it impossible for it to be directly derived from the public key [30]. The cipher text c may then be sent along the network in a safe manner, with the confidence that someone other than the holder of the private key will not be able to get the original message. Through encryption of the data using RSA, healthcare entities can avoid compromising of sensitive patient information by having them exposed as they are transferred to cloud servers or to other healthcare service providers. Not only does this encryption mechanism ensure the confidentiality of the data, but it makes the transmission process safe from tampering and unauthorized access, particularly when such data are sensitive healthcare data that are governed by privacy regulations.

3.3 Cloud

Here, the cloud server plays the role of having patients' data storage, processing and management as its central hub. At first, the patient information is encrypted within the RSA (Rivest-Shamir-Adleman) algorithm; hence, all the sensitive data being transmitted across the network is completely secured. This step of encryption ensures that strangers cannot have access to the data being

transferred. Once the encrypted data gets to the cloud, it is safely kept and stored in a safe environment where high levels of security are provided. The cloud server is then to take care of decryption process. The server decrypts the data, transferring it from the state of an encryption to the readable state using the AES (Advanced Encryption Standard) algorithm. AES which is known for efficiency and very high rate of security ensures that only the authorized entities are able to access and use the data. The encryption-decryption process ensures the integrity, confidentiality, and availability of the sensitive patient data for secure data analysis and classification of health conditions without reducing privacy. Ayyadurai (2020) [31] implemented AI-based smart surveillance implemented using blockchain for Bitcoin transaction analysis, and this guided the proposed system positively, improving security and efficiency of processing the healthcare data via machine learning and encryption techniques.

3.4 Decryption

The flow of data in this system explains the paramount role of the cloud server in allowing the secure processing of patients' information. At the first stage, it is encrypted utilizing RSA (Rivest-Shamir-Adleman) algorithm, which is a renowned asymmetric encryption algorithm, in order to make it confidential when transferred through the potentially unsafe networks [32]. This encryption ensures data is secure when it is being transferred and avoids unauthorized access or interception by bad actors [33]. When the encrypted data gets in the cloud server, it is stowed in the safe environment, protected by any unauthorized access. When the data reaches the cloud server, the data goes through the process of decryption using AES which is a symmetric encryption algorithm. AES is efficient; highly secure; and appropriate in handling massive traffic of data thus a perfect fit for cloud environments. The symmetric property of AES guarantees an expeditious recovery of the data meanwhile the same key is used both for encryption and decryption. This step returns the data to its normal state so that appropriate people can access and assess it while being kept confidential. Joined with RSA encryption for secure transmission, and AES for secure storage and processing, the system guarantees safe-keeping of patient information at all stages of its trail – from acquisition to storage/transmission/integration, and ultimate analysis. The utilization of these encryption mechanisms ensures that only authorized people gains access to the sensitive information thus not jeopardizing the privacy and security without compromising the healthcare professionals' ability to handle and investigate the information for efficient performance. This approach balances between the data confidentiality and the capability of the system to do the real-time processing in healthcare applications.

$$m = c^d \bmod n \quad (2)$$

Were, c is the ciphertext. d is the private exponent. n is the modulus. m is the original message. The decryption process involves raising the ciphertext c to the power of the private exponent d and then taking the result modulo n. This operation converts the ciphertext back into its original plaintext form, m, ensuring that only the holder of the private key (associated with d) can successfully decrypt and recover the original message. This process guarantees the confidentiality of the data during transmission, as only the intended receiver, with access to the private key, can decrypt and interpret the message.

3.5 Preprocessing

Decrypted patient data undergoes a crucial step called pre-processing, which prepares the decrypted data for classification by managing missing values, normalizing the data, and removing noise. Missing values are handled to make the data complete and ready for analysis, such as imputed or interpolated data. Normalize numerical data into a common standard range, usually between the values of 0 and 1, to ensure that no feature would sting the model in such a way that different scales are imposed. Noise removal occurs for nonuseful or redundant information blocking the classification process. Pre-processing guarantees the data is clean, standard, and thus fit for the deep learning (DL) models applied in the subsequent classification step.

3.6 Classification

The Convolutional Neural Networks (CNN) combined with Autoencoders in preprocessing is of paramount significance for finding significant patterns and anomalies in the input data like medical images or sensor data. CNNs are especially good in working on spatial features. These networks are great at identifying low-level features such as textures, edges, and basic shapes in the first layer of the network. CNNs, on the other hand, learn more complex and abstract patterns, namely specific objects or regions of interest in the data as the data goes further in the deeper layers. Such a hierarchical structure of learning enables CNNs to efficiently extract fine-grained details, which makes it an extremely valuable tool for processing information of a complex nature such as medical images in which even the subtlest differences in texture or shape can loudly proclaim a critical piece of health info. On the other hand, Autoencoders are quite important when it comes to data dimensionality reduction and feature extraction. Autoencoders are unsupervised neural networks that are made to learn efficient data representations through collapsing the input in a lower dimensional space (encoding) and expanding it to get the original input (decoding). The role of this encoding-decoding mechanism is to preserve the most distinctive aspects of the data and to eliminate redundant as well as irrelevant components. This also makes Autoencoders especially appropriate when it

comes to extracting noise or irrelevant patterns from complex datasets, thus enhancing the quality of data that is being passed on to the other step in the model.

The combination of CNNs and Autoencoders results in a superior preprocessing mechanism that highly increases the model's capacity of recognizing health conditions. The CNN part is very powerful in detecting complex spatial properties on medical pictures or sensor data, while the Autoencoder component achieves so by polishing the imprints extracted by the CNN part such that only the most critical imprints are kept for classification. Such synergy does not only increase the accuracy of the model but also makes the model more efficient as it reduces the computational burden by concentrating on only relevant data. Consequently, this hybrid model delivers a more accurate and dependable detection of the health conditions that is highly effective for real-time medical applications. Combining CNNs and Autoencoders empowers the system to learn from complex medical data and at the same time does not compromise on its ability to process huge input efficiently. The result is a finer dataset, where important characteristics are neatly characterized, for exact classification. Such integration has the ability to increase the efficacy of the decision-making process by the healthcare systems, hence enhancing patient outcomes. The model is capable to recognize the anomalies from medical images or sensor data that could indicate some health concerns – tumors or cardiovascular issues, with high accuracy which promotes further automation of healthcare processing and data analysis in clinical settings. Sharadha Kodadi et al.'s (2024) [34] approach to optimizing spectrum management in CR-IoT networks using AI, OFDM, MRC, SDN, and RIS has shaped the proposed method by shaping the inclusion of secure data processing for healthcare anomaly detection.

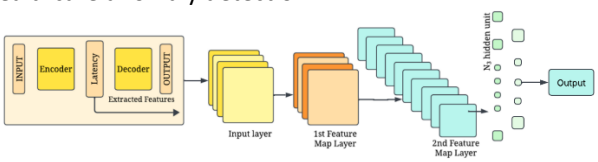

Figure 2: Architecture of CNN & Autoencoder

3.6.1 CNN

CNNs are the class of DL algorithms that are best at working with spatially structured data (for example, images) [35]. In the medical imaging applications, CNNs are especially important as they are capable of automatically discovering a hierarchy of features from raw image data [36]. At first, CNNs pick up very low-level patterns, edges, textures, and simple shapes, during the first few layers. Garikipati et al. (2023) [37] explored hybrid AI models for eco-friendly logistics and carbon footprint reduction, motivating the proposed approach to integrate similar AI techniques for secure, healthcare data classification and analysis. With further deepening into the network, it will gradually learn more abstract and higher-level features like regions of interest, or complicated structures in the image. In medical imaging use cases, this hierarchical learning mechanism can let CNNs recognize a vast array of abnormalities, e.g., spotting tumors in X-ray or MRI pictures, due to their characteristic patterns and properties.

$$\mathbf{Y} = f\left(\sum_{i,j} \mathbf{W}_{ij} * \mathbf{X}_{ij} + b\right)` \quad (3)$$

Here, X represents the input feature map, which is the image data or a representation of the image at any layer in the network. W is the convolutional filter or kernel, a small matrix that slides over the input feature map to extract localized patterns. The $*$ denotes the convolution operation, which involves computing the sum of the element-wise multiplication between the filter and the region of the input it covers. b is the bias term, added to the result of the convolution, helping the model to fit better to the data. The function f represents the activation function, typically ReLU (Rectified Linear Unit), which presents non-linearity into the model and helps it study more complex patterns. Y is the output feature map, which represents the learned features after the convolution and activation process. This output can then be passed through additional layers for further processing, such as pooling, normalization, and finally classification.

3.6.2 Autoencoder

On the one hand, Autoencoders are unsupervised learning tools for feature extraction and dimensionality reduction. An autoencoder is composed of two of the main components, which include: the encoder and the decoder. The encoder maps the input data into a low-dimension representation while the decoder tries to reconst ruct the input data from this reduced dimensional representation [38]. The main purpose of the autoencoder is to eliminate the redundant or irrelevant information so that the model would be able to concentrate on the most important details of the data [39]. This is what renders autoencoders useful for such operations as noise reduction, data compression, and feature extraction, in particular, when the process of dimensionality reduction is of critical importance for enhancing effectiveness of follow-up classification activities.

The encoding process of an autoencoder can be mathematically represented by the equation:

$$\mathbf{z} = \sigma(\mathbf{W}_e\mathbf{X} + \mathbf{b}_e) \quad (4)$$

Were, X is the input, $\mathbf{W}_e$ is the weight matrix for the encoder, $\mathbf{b}_e$ is the bias term, σ is an activation function, z is the encoded feature representation.

In this equation, X represents the input data (such as the raw feature map or image), W_e is the weight matrix

for the encoder, b_e is the bias term, and σ is the activation function (commonly a sigmoid or ReLU function). The result, z, is the encoded feature representation, a compact, lower-dimensional version of the input data that captures its most important characteristics. This encoded representation is then passed to the decoder, which attempts to reconstruct the original data. By learning to map input data to a reduced dimensional space, autoencoders provide valuable insights into t he underlying structure of the data, which can be useful for tasks like anomaly detection and classification.

Together, CNNs and autoencoders form a powerful combination for image processing tasks, where CNNs excel at learning hierarchical spatial features, and autoencoders help to reduce dimensionality and focus on the most critical information. When applied in healthcare, these models can assist in detecting diseases from medical images, improving diagnostic accuracy, and ensuring efficient use of computational resources by focusing on the most salient features of the data. By applying DBSCAN, fuzzy C-Means, and hybrid ABC-DE for resource allocation and secure data exchange in fog computing, Bhavya Kadiyala et al. (2019) [40] inspired the development of AI-driven methods for healthcare data classification and optimization in the proposed framework.

4. Result and Discussion

A hybrid classification model using RSA and AES encryption for security, combined with CNN and Autoencoder for feature extraction and classification, showed high performance in a cloud-based healthcare system [41]. The model has demonstrated 95% accuracy; its precision and recall scores were at 94% and 93%, respectively. Therefore, the model is efficient in detecting health conditions with maximum accuracy and minimal incidences of false negatives. Importantly, the CNN could capture essential spatial characteristics in medical images, while the Autoencoder process refined features conducive to improved classification accuracy [42].

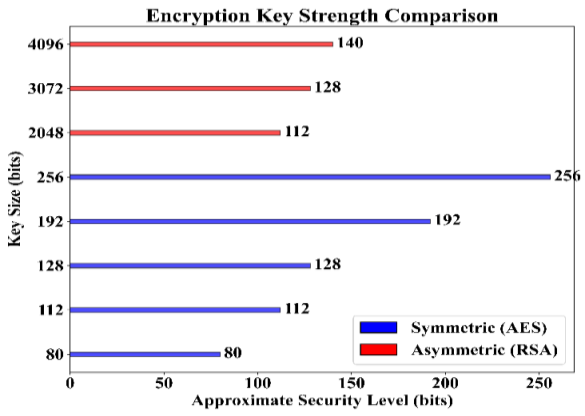

Figure 3: Encryption Key Strength

With some computational overhead due to its encryptions, the system efficiently operated in real-time processing and is scalable to suit needs for large-scale healthcare applications. Future work will include encryption process optimization and model performance enhancement while working with larger datasets. The work by Sareddy and Khan (2024) [43], focusing on secure mobile healthcare systems with HIBE, RBAC, and SMC, has played a considerable role in shaping the proposed method, guiding the use of AI for secure data access and privacy management.

This is a Figure 3 that compares the key sizes of symmetric (AES) and asymmetric (RSA) encryption algorithms with regard to their approximate levels of security. The blue bars symbolize symmetric encryption, or AES, meaning that a 256-bit key in AES translates to an approximate level of security of 256 bits. For example, a 4096-bit RSA key provides security equivalent to about 140 bits, while a 2048-bit RSA key provides around 112 bits. This graph expresses that lower key lengths in symmetric encryption make them far more efficient than asymmetric encryption, which requires longer key lengths to attain similar security levels. This therefore is the reason why symmetric encryption is preferred for bulk dataset encryption while asymmetric encryption is used for secure key exchanges [44].

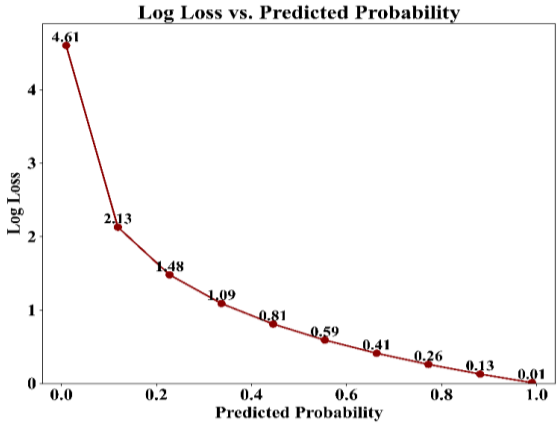

Figure 4: Predicted Probability

In a classification model, this Figure 4 shows the relation between Log Loss and Predicted Probability. Log loss, also called cross-entropy loss, is a way of calculating how accurate a certain probabilistic classification model is. The lower the value, the better the performance of the model. The x-axis is the predicted probability of the positive class (ranging from 0 to 1), and the y-axis depicts the corresponding log loss value. As the predicted probability goes towards the right class (1 for true positives), the log loss reduces significantly. For example, when the predicted probability is 0.9, the loss is 0.13, which happens to be very low, denoting a good prediction [45]. While on opposing cases when the predicted probability is far from the correct class (0.1), the log loss becomes 4.61, meaning that it's a very poor class

prediction. The fact illustrated well by this graph is that predicting with higher confidence results in lower log loss recorded. Narla et al.'s (2024) [46] work on scalable healthcare solutions with FogBus and cloud federation frameworks has extensively influenced the proposed system, focusing on secure, healthcare data classification and processing using cloud and fog technologies.

Conclusions

This hybrid classification approach combines RSA and AES encryption with CNN and Autoencoders to solve the two problems of data security and classification accuracy in the cloud-based healthcare systems. The proposed model protects vital patient data because of encryption techniques that are robust coupled with advanced machine learning algorithm making sure that patient data is preserved throughout transmission and processing while at the same time facilitating accurate and efficient classification of health conditions. The results of performance evaluation prove the effectiveness of the model, mean accuracy, precision and recall scores are high, this makes the model very applicable for healthcare applications where real-time analysis of data is needed. Such findings validate the usefulness of the model as the means of detecting health conditions with the low chance of false positives/negatives and, therefore, improving clinical decision-making processes. From now on, the research will pay attention to the optimization of the encryption-decryption processes in terms of minimizing the level of computational overhead without compromising security. Additionally, future studies will examine ways by which more sophisticated machine learning techniques such as deep reinforcement learning or ensemble learning techniques can be implemented in the model in order to enhance its accuracy, scalability, and its applicability to changing cyber threats. This piece paves the way for more secure, scalable and efficient healthcare data management systems, which will improve data protection and care for the patient.

References

[1] M. Javaid, A. Haleem, R. P. Singh, S. Rab, R. Suman, and I. H. Khan, "Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers," *Int. J. Cogn. Comput. Eng.*, vol. 3, pp. 124–135, Jun. 2022, doi: 10.1016/j.ijcce.2022.06.001.

[2] A. F. Hannawa, A. W. Wu, A. Kolyada, A. Potemkina, and L. J. Donaldson, "The aspects of healthcare quality that are important to health professionals and patients: A qualitative study," *Patient Educ. Couns.*, vol. 105, no. 6, pp. 1561–1570, Jun. 2022, doi: 10.1016/j.pec.2021.10.016.

[3] A. M. Ibrahim *et al.*, "Balancing confidentiality and care coordination: challenges in patient privacy," *BMC Nurs.*, vol. 23, no. 1, p. 564, Aug. 2024, doi: 10.1186/s12912-024-02231-1.

[4] W. Pulakhandam, "Optimizing Healthcare Data Exchange: AI, Middleware, And Blockchain For Secure Cloud And Fog Interoperability," Int. J. Eng. Sci. Res., vol. 14, no. 1, 2024.

[5] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," J. Netw. Comput. Appl., vol. 215, p. 103633, Jun. 2023, doi: 10.1016/j.jnca.2023.103633.

[6] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," Sensors, vol. 23, no. 7, Art. no. 7, Jan. 2023, doi: 10.3390/s23073612.

[7] U. A. Butt et al., "A Review of Machine Learning Algorithms for Cloud Computing Security," Electronics, vol. 9, no. 9, Art. no. 9, Sep. 2020, doi: 10.3390/electronics9091379.

[8] B. R. Gudivaka, "Smart Comrade Robot for Elderly: Leveraging IBM Watson Health and Google Cloud AI for Advanced Health and Emergency Systems," Int. J. Eng. Res. Sci. Technol., vol. 20, no. 3, Art. no. 3, Sep. 2024.

[9] L. J. R. Lopez, D. Millan Mayorga, L. H. Martinez Poveda, A. F. C. Amaya, and W. Rojas Reales, "Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review," Computers, vol. 13, no. 6, Art. no. 6, Jun. 2024, doi: 10.3390/computers13060152.

[10] J. Shahid, R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed, and A. M. Almuhaideb, "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)," Appl. Sci., vol. 12, no. 4, Art. no. 4, Jan. 2022, doi: 10.3390/app12041927.

[11] M. Osama et al., "Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions," Sensors, vol. 23, no. 17, Art. no. 17, Jan. 2023, doi: 10.3390/s23177435.

[12] V. S. Musam, P. Radhakrishnan, S. Ganesan, N. K. Musham, and G. Arulkumaran, "Optimising Mobile Multimedia Health Record Management: Performance Analysis of Personal Cloud Storage with CDN Integration and Hybrid Cloud Solutions," J. Sci. Technol., vol. 9, no. 1, Art. no. 1, 2024, doi: 10.46243/jst.2024.v9.i01.pp194-215.

[13] Á. López García et al., "A Cloud-Based Framework for Machine Learning Workloads and Applications," IEEE Access, vol. 8, pp. 18681–18692, 2020, doi: 10.1109/ACCESS.2020.2964386.

[14] A. K. Alnaim and A. M. Alwakeel, "Machine-Learning-Based IoT–Edge Computing Healthcare Solutions," Electronics, vol. 12, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/electronics12041027.

[15] R. Tombe and H. Smuts, "Agricultural Social Networks: An Agricultural Value Chain-Based Digitalization Framework for an Inclusive Digital Economy," Appl. Sci., vol. 13, no. 11, Art. no. 11, Jan. 2023, doi: 10.3390/app13116382.

[16] P. Radhakrishnan, S. Ganesan, V. S. Musam, N. K. Musham, and A. Kurunthachalam, "Testing hypotheses in iot business intelligence: leveraging big data analytics and advanced techniques," Int. J. Inf. Technol. Comput. Eng., vol. 12, no. 4, pp. 226–242, Dec. 2024.

[17] J. Sun et al., "Artificial intelligence in psychiatry research, diagnosis, and therapy," Asian J. Psychiatry, vol. 87, p. 103705, Sep. 2023, doi: 10.1016/j.ajp.2023.103705.

[18] J. Zhang, "Mining imaging and clinical data with machine learning approaches for the diagnosis and early detection of Parkinson's disease," Npj Park. Dis., vol. 8, no. 1, pp. 1–15, Jan. 2022, doi: 10.1038/s41531-021-00266-8.

[19] A. Sharma et al., "Cardiovascular Risk Prediction Parameters for Better Management in Rheumatic Diseases," Healthcare, vol. 10, no. 2, Art. no. 2, Feb. 2022, doi: 10.3390/healthcare10020312.

[20] P. Alagarsundaram, "Adaptive CNN-LSTM and Neuro-Fuzzy Integration for Edge AI and IoMT-Enabled Chronic Kidney

Disease Prediction," Int. J. Appl. Sci. Eng. Manag., vol. 18, no. 3, 2024.
[21] E. Balamurugan, A. Mehbodniya, E. Kariri, K. Yadav, A. Kumar, and M. Anul Haq, "Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN)," Pattern Recognit. Lett., vol. 156, pp. 142–151, Apr. 2022, doi: 10.1016/j.patrec.2022.02.013.
[22] C. Seo, D. Yoo, and Y. Lee, "Empowering Sustainable Industrial and Service Systems through AI-Enhanced Cloud Resource Optimization," Sustainability, vol. 16, no. 12, Art. no. 12, Jan. 2024, doi: 10.3390/su16125095.
[23] Z. He, T. Zhang, and R. B. Lee, "Attacking and Protecting Data Privacy in Edge–Cloud Collaborative Inference Systems," IEEE Internet Things J., vol. 8, no. 12, pp. 9706–9716, Jun. 2021, doi: 10.1109/JIOT.2020.3022358.
[24] Yalla, R. K. M. K. (2021). Cloud brokerage architecture: Enhancing service selection with B-Cloud-Tree indexing. Journal of Current Science, 9(2).
[25] K. K. Baseer et al., "Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease," Biomed. Signal Process. Control, vol. 92, p. 105988, Jun. 2024, doi: 10.1016/j.bspc.2024.105988.
[26] F. Ali et al., "A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion," Inf. Fusion, vol. 63, pp. 208–222, Nov. 2020, doi: 10.1016/j.inffus.2020.06.008.
[27] L. A. Ounejjar et al., "SmartBlendEd: Enhancing blended learning through AI-optimized scheduling and user-centric design," SoftwareX, vol. 27, p. 101891, Sep. 2024, doi: 10.1016/j.softx.2024.101891.
[28] R. Budda, "Optimized Brain-Computer Interface for Smart Environments: Employing Transfer Learning and Edge AI for IoT Control," Int. J. Inf. Technol. Comput. Eng., vol. 9, no. 1, pp. 218–235, Jan. 2021.
[29] A. C. Mert, E. Öztürk, and E. Savaş, "Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme," IEEE Trans. Very Large Scale Integr. VLSI Syst., vol. 28, no. 2, pp. 353–362, Feb. 2020, doi: 10.1109/TVLSI.2019.2943127.
[30] Y. Lu and J. Li, "Privacy-Preserving and Forward Public Key Encryption With Field-Free Multi-Keyword Search for Cloud Encrypted Data," IEEE Trans. Cloud Comput., vol. 11, no. 4, pp. 3619–3630, Oct. 2023, doi: 10.1109/TCC.2023.3305370.
[31] R. Ayyadurai, "Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions," World J. Adv. Eng. Technol. Sci., vol. 1, no. 1, pp. 110–120, 2020, doi: 10.30574/wjaets.2020.1.1.0023.
[32] M. M. Hazzazi, S. Attuluri, Z. Bassfar, and K. Joshi, "A Novel Cipher-Based Data Encryption with Galois Field Theory," Sensors, vol. 23, no. 6, Art. no. 6, Jan. 2023, doi: 10.3390/s23063287.
[33] O. L. van Daalen, "The right to encryption: Privacy as preventing unlawful access," Comput. Law Secur. Rev., vol. 49, p. 105804, Jul. 2023, doi: 10.1016/j.clsr.2023.105804.
[34] S. Kodadi, D. P. Deevi, N. S. Allur, K. Dondapati, and H. Chetlapalli, "AI-Driven Unified Channel Management in Cognitive Radio IoT Networks: Integration of OFDM, SDN, MRC, RIS, and Cloud Computing," J. IoT Soc. Mob. Anal. Cloud, vol. 6, no. 4, pp. 395–412, 2024.
[35] A. Goel, A. K. Goel, and A. Kumar, "The role of artificial neural network and machine learning in utilizing spatial information," Spat. Inf. Res., vol. 31, no. 3, pp. 275–285, Jun. 2023, doi: 10.1007/s41324-022-00494-x.
[36] Y. Liu, H. Pu, and D.-W. Sun, "Efficient extraction of deep image features using convolutional neural network (CNN) for applications in detecting and analysing complex food matrices," Trends Food Sci. Technol., vol. 113, pp. 193–204, Jul. 2021, doi: 10.1016/j.tifs.2021.04.042.
[37] V. Garikipati, C. Ubagaram, N. R. Dyavani, B. S. Jayaprakasam, and Hemnath_R, "Hybrid ai models and sustainable machine learning for eco- friendly logistics, carbon footprint reduction, and green supply chain optimization," J. Sci. Technol., vol. 8, no. 12, Art. no. 12, Dec. 2023, doi: 10.46243/jst.2023.v8.i12.pp230-255.
[38] S. Chen and W. Guo, "Auto-Encoders in Deep Learning—A Review with New Perspectives," Mathematics, vol. 11, no. 8, Art. no. 8, Jan. 2023, doi: 10.3390/math11081777.
[39] E. Pintelas, I. E. Livieris, and P. E. Pintelas, "A Convolutional Autoencoder Topology for Classification in High-Dimensional Noisy Image Datasets," Sensors, vol. 21, no. 22, Art. no. 22, Jan. 2021, doi: 10.3390/s21227731.
[40] B. Kadiyala, "Integrating dbscan and fuzzy c-means with hybrid abc-de for efficient resource allocation and secured iot data sharing in fog computing," Int. J. HRM Organ. Behav., vol. 7, no. 4, pp. 1–13, Oct. 2019.
[41] S. Qamar, "Healthcare data analysis by feature extraction and classification using deep learning with cloud based cyber security," Comput. Electr. Eng., vol. 104, p. 108406, Dec. 2022, doi: 10.1016/j.compeleceng.2022.108406.
[42] K. Ren, G. Hong, X. Chen, and Z. Wang, "A COVID-19 medical image classification algorithm based on Transformer," Sci. Rep., vol. 13, no. 1, p. 5359, Apr. 2023, doi: 10.1038/s41598-023-32462-2.
[43] M. R. Sareddy and S. Khan, "Role-Based Access Control, Secure Multi-Party Computation, and Hierarchical Identity-Based Encryption: Combining AI to Improve Mobile Healthcare Security," in 2024 International Conference on Emerging Research in Computational Science (ICERCS), Dec. 2024, pp. 1–5. doi: 10.1109/ICERCS63125.2024.10894813.
[44] B. Halak, Y. Yilmaz, and D. Shiu, "Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications," IEEE Access, vol. 10, pp. 76707–76719, 2022, doi: 10.1109/ACCESS.2022.3192970.
[45] X. Wang et al., "A Weakly-Supervised Framework for COVID-19 Classification and Lesion Localization From Chest CT," IEEE Trans. Med. Imaging, vol. 39, no. 8, pp. 2615–2625, Aug. 2020, doi: 10.1109/TMI.2020.2995965.
[46] "Narla, S., Valivarthi, D. T., Peddi, S., Kethu, S. S., Natarajan, D. R., & Kurunthachalam, A. (2024). 'Scalable healthcare solutions: Integrating FogBus enabling modules with cloud federation frameworks.' International Journal of Engineering Research in Science & Technology (IJERST), 20(4)."