CHAPTER SIX

A smart healthcare system using IoT and machine learning

Roseline Oluwaseun Ogundokun[a,b,c], Muhtahir Oluwaseyi Oloyede[d], Hakeem Babalola Akande[e], Julius Olaniyan[a], Deborah Olaniyan[a], and Chinecherem Umezuruike[f]

[a]Department of Computer Science, Landmark University Omu Aran, Omu Aran, Kwara State, Nigeria
[b]Department of Computer Systems Engineering, Tshwane University of Technology (TUT), Pretoria, South Africa
[c]Department of Centre of Real Time Computer Sciences, Kaunas University of Technology, Kaunas, Lithuania
[d]Department of Information Technology, University of Ilorin, Ilorin, Kwara State, Nigeria
[e]Department of Telecommunication Science, University of Ilorin, Ilorin, Kwara State, Nigeria
[f]Department of Software Engineering, Bowen University Iwo, Iwo, Osun State, Nigeria

Contents

Abstract

Integration of the Internet of Things (IoT) and Machine Learning (ML) in smart healthcare systems presents new possibilities for better patient care and administration. However, it also raises concerns about privacy, trust, and security. This research aims to establish a complete framework that addresses these challenges, with the overall goal of maintaining the dependability and secrecy of smart healthcare. The study presents a system architecture that includes integrated data, data preprocessing, model

Advances in Computers, Volume 137
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2024.06.008

design and training Long-Short Term Memory with Attention Mechanism (LSTM-AM), and cloud-based validation. It draws on a synthesized dataset of 5000 hospital user profiles. Rigorous training and validation confirm the system's outstanding efficiency, resulting in 99.06% accuracy, 98.14% precision, 99.06% recall, and a 99.00% F1 score. Consequently, this demonstrates that the approach handles healthcare data safely and confidentially. There is a considerable improvement in sequential data processing when LSTM-AM is used and cloud validation is utilized to maintain data integrity. This work introduces an innovative strategy to integrate IoT and ML in healthcare, addressing security and privacy concerns and potentially revolutionizing patient care and administration. The study will assist physicians in the diagnosis and treatment of patient diseases securely, privately and more accurately.

1. Introduction

The rapid expansion of Smart Healthcare Systems (SHS) in recent years has cemented their status as indispensable elements of the contemporary economy. A key enabler of this growth has been the Internet of Medical Things (IoMT), which facilitates the development of various applications such as telemedicine, medication management, and remote medical monitoring [1–4]. IoMT encompasses devices embedded with sensors and interconnected within the healthcare industry, offering solutions to enhance patient care while alleviating the burdens on healthcare institutions [5–8]. However, this proliferation of IoMT technology has simultaneously raised concerns about healthcare data security, privacy, and trustworthiness [9–11]. The protection of data integrity, authenticity, and confidentiality has become paramount, preserving patient privacy amidst evolving threats and vulnerabilities. Despite using encryption techniques and cloud-based security solutions, challenges persist in ensuring robust data protection and maintaining trust in the ML models employed within healthcare settings [12]. These challenges underscore the urgent need for Privacy-Preserving Machine Learning (PPML) in healthcare to rectify deficiencies and fortify existing systems against potential breaches and misuse. The primary objective of this study is to address these pressing concerns by proposing a comprehensive framework that integrates IoT and ML technologies within smart healthcare systems. This framework is designed to address privacy, trust and security issues effectively, offering a systematic approach to managing healthcare data while maintaining confidentiality and integrity. The proposed solution includes the development of a robust system architecture validated through rigorous assessment methodologies, ensuring its reliability and effectiveness in the secure handling of healthcare data.

Furthermore, the study introduces innovative approaches to seamlessly integrating IoT and ML within healthcare settings, using advanced ML techniques like LSTM-AM to improve prediction accuracy and instill greater confidence in healthcare services. Putting emphasis on the critical need for PPML, the report outlines recent advances in this area and highlights its potential to address evolving privacy challenges. Ultimately, the trusted, envisioned smart healthcare services aim to revolutionize patient care by effectively addressing existing issues and streamlining administrative processes. The project aims to advance smart healthcare systems and meet vital demands in an increasingly technology-driven healthcare landscape by confronting security, privacy and trust management challenges through IoT and ML technologies.

The problem revolves around the security, privacy, and trust management challenges inherent in SHS that use IoMT technology. Despite the significant advances facilitated by IoMT, such as telemedicine and remote monitoring, its widespread adoption has brought about a host of vulnerabilities and risks [13,14]. Vulnerabilities in IoMT devices pose a threat of unauthorized access to critical healthcare data, raising concerns about potential data breaches. Current security measures often do not protect personal information effectively, leading to privacy issues, as attackers can exploit weaknesses to access sensitive health data [15,16]. Furthermore, the trustworthiness of ML models used in healthcare settings is compromised due to doubts regarding the accuracy and transparency of their predictions. These challenges highlight the urgent need for PPML solutions tailored to the unique requirements of the healthcare sector.

Existing solutions to the security, privacy and trust management challenges in SHS that take advantage of IoMT technology include encryption techniques, cloud-based security solutions and privacy-enhancing technologies. Although these approaches aim to mitigate risks associated with unauthorized access and data breaches, they have significant limitations. Encryption methods, though widely used, may be vulnerable to sophisticated attacks and require robust key management. Cloud-based solutions offer scalability but raise concerns about data sovereignty and compliance. Privacy-enhancing technologies provide promising solutions, but often have computational overhead and interoperability challenges. Furthermore, ensuring the trustworthiness of ML models in healthcare remains critical due to concerns about transparency, bias, and accountability. Addressing these challenges requires a comprehensive approach that balances usability, effectiveness, and regulatory compliance to secure healthcare data and foster trust in smart healthcare systems.

The scheme proposed in this chapter addresses the security, privacy and trust management challenges inherent in SHS utilizing IoMT technology. It presents a comprehensive framework that integrates IoT and ML technologies within SHS to address these issues effectively. The scheme focuses on developing a robust system architecture to manage healthcare data while maintaining confidentiality and integrity efficiently. It emphasizes the necessity for PPML to ensure the safe and efficient use of IoT and ML technology in healthcare. Advanced ML techniques such as LSTM-AM are used to enhance prediction accuracy and instill greater confidence in healthcare services. Furthermore, the scheme aims to introduce safe, private and easy-to-use smart healthcare services, ultimately revolutionizing patient care and administrative processes in healthcare settings. The main contributions of the chapter are outlined as follows:

1. This chapter combines IoMT and ML techniques to improve the security of healthcare data.
2. The proposed approach supports user-friendly healthcare services and uses LSTM-AM to enhance predictions.
3. Results and discussion show the efficiency of the proposed approach compared to ither state-of-the-art approaches.

The chapter is structured as follows: Section 2 discusses the related works, while problem statements are presented in Section 3. The system model and the design are also discussed in Section 3. Section 4 presents the proposed scheme and the algorithms employed in this study are presented. The generation and pre-processing of the dataset used in this study are presented along with the model design, training, and validation. The proposed model performance analysis is presented in Section 5. This included discussing the experimental environment, describing the data set used in the study, presenting the results and discussing the experiment conducted. The study was conducted in Section 6, and future works were also recommended.

2. Related works

Rani et al. [17] devised a technique to securely transmit data on the IoMT, focusing on selecting the most appropriate users. This method utilizes the Chinese Remainder Theorem to produce encrypted data for a specified number of users and incorporates a metaheuristic algorithm for determining users. The simulation results highlighted the method's efficacy in computational time and energy expenditure. Although the strategy is effective in ensuring security for IoT-based smart home systems, it has some limitations in terms of security.

Alabdulkarim et al. [18] introduced a method to protect privacy in clinical Decision Support Systems (DSS). Their approach involves using a single Decision Tree (DT) to diagnose symptoms while ensuring patient data remains secure from network threats. The technology employs homomorphic encryption and nonces to safeguard user data and thwart one-sided decryption. While the system outperforms the Naïve Bayes method by 46.46% in simulations, it does have drawbacks in the context of security services.

Boussada et al. [19] conducted a study on a data transmission method that prioritizes privacy in Smart Home Systems enabled by the IoMT. The system employs user pseudonyms as public keys and is built upon lightweight Identity-based encryption using the Elliptic Curves Discrete Logarithm (ECDL) technique. The system's performance analysis demonstrates its efficacy while adhering to contextual and content privacy standards. However, it is unsuitable for emergency electronic healthcare situations.

Gull et al. [20] proposed a reversible data concealment method that utilizes dual pictures for IoMT networks. The technique uses Huffman encoding to preprocess confidential data and then incorporates them into two visually identical images. Although the method guarantees a high level of perceptual quality while accommodating a large amount of data, it does not have an efficient approach for handling underflow and overflow problems.

Huang et al. [21] presented a pragmatic approach to verifying the identity of patients using distorted Electrocardiogram (ECG) data while still guaranteeing privacy. The technique adjusts its algorithm according to the current mobility state and ensures the confidentiality of the ECG templates by making them indistinguishable. Although the system has been shown to be successful and verified on online datasets and human subjects, it lacks adaptability in its ability to protect against threats.

Xu et al. [22] propose a five-layer architecture to monitor and managing the health of manufacturing workers. They analyze the system's implementation process, which includes processing environmental data, monitoring physical conditions, providing system services and management, and presenting the corresponding algorithms.

In Ref. [23], Lin and Xu [23] proposes a method to remotely monitor users' health and identify ailments. They suggest a new network of areas of the human body to analyses brain illnesses. This network involves collecting initial data, correcting data, transmitting data, and performing complete data analyses to ensure the output of the analysis is of high quality. Given the wide range of available options, patients are curious about selecting antihypertensive medications suitable for their needs.

The paper "BPatient State Recognition System for Healthcare Using Speech and Facial Expressions" by Hossain [24] proposes a patient state recognition system for the healthcare framework that offers high recognition accuracy, cost-effective modeling, and scalability. The system accepts two primary forms of input: video and audio, both recorded in a multisensory setting. Presenting body postures using equations of the skeletal system and achieving long-term physical rehabilitation, taking into account the unique features of each individual, is a challenging research problem. In the study titled "An Intelligent Body Posture Analysis Model Using Multiple Sensors for Long-Term Physical Rehabilitation," Lai et al. [25] introduce a new approach called the "Intelligent Body Posture Analysis Model." This method utilizes numerous acceleration sensors and gyroscopes to identify patterns in body movements. Neonatal jaundice is a prevalent disease that arises in newborns during the first week of their existence.

Aydın et al. [26] suggested a non-intrusive device to monitor and detecting jaundice at regular intervals, helping clinicians in early diagnosis. The revised Wechsler Adult Intelligence Scale is a commonly used assessment tool designed to evaluate and categorize adults' cognitive abilities wholly and thoroughly. The article titled "BRank Determination of Mental Functions by 1D Wavelets and Partial Correlation" was authored by Karaca et al. [27]. Their study provides a methodology that uses wavelets and correlation analysis to categorize mental functioning. ECG monitoring is extensively researched and used as a crucial method of diagnosing cardiac problems.

In Ref. [28], Yang et al. [28] presents a novel ECG monitoring approach with IoT methods. The method involves collecting ECG data via a wearable monitoring node and transmitting them directly to the IoT cloud over Wi-Fi. Assess the disparity between and between groups of young people with the motions executed by a therapist. In their study "Variability analysis of Therapeutic Movements using wearable inertial sensors", Lopez-Nava et al. [29] analyze five upper arm therapy motions performed by young people without mobility impairments. Movements are compared to reference data provided by therapists. In Ref. [30], human generic intellectual tasks are examined. They propose an integrated modeling framework to represent a medical Cyber-Physical-Human system (CPH System) and utilize UPPAAL as the underlying foundation for integration. Table 1 briefly explains the objectives, methods, contributions, and limitations of each work related to IoMT security and privacy in smart healthcare systems.

Table 1 Summary of related works.

Scheme	Key findings	Advantages	Disadvantages
[17]	Secure data transmission in IoMT	Enhanced computation time and energy efficiency in data security	Offers limited security
[18]	Privacy in clinical DSS	Superior performance to Naive Bayes algorithm; protects data privacy	Limited security services
[19]	Privacy-aware data transmission for IoMT	Meets privacy requirements; effective in limited resource environments	Not suitable for emergency e-healthcare
[20]	Extensive capacity data hiding for IoMT networks	High perceptual quality with large payload	Ineffective in managing underflow and overflow issues
[21]	Validate patients with ECG signals, privacy protection	Effective authentication and privacy protection; validated on datasets	Lacks flexibility against attacks
[22]	Propose a five-layer architecture for monitoring and managing the health of manufacturing workers	Introduce a comprehensive approach to health monitoring for manufacturing workers	Lack of detailed discussion on the effectiveness and real-world implementation of the proposed architecture
[23]	Develop a human body area network for remote health monitoring and brain disease analysis	Present a novel approach to the analysis and remote health monitoring	There is limited discussion on the scalability and practical implementation of the proposed network
[24]	Design a patient state recognition system for the healthcare framework	Offer a cost-effective and scalable solution for patient state recognition in healthcare	There is a lack of discussion on the system's adaptability to different healthcare environments and patient demographics

Continued

Table 1 Summary of related works.—cont'd

Scheme	Key findings	Advantages	Disadvantages
[25]	Introduce an intelligent body posture analysis model for long-term physical rehabilitation	Propose an innovative approach to long-term physical rehabilitation through posture analysis	Limited discussion on the practical implementation and integration of the proposed model into existing rehabilitation practices
[26]	Develop a non-intrusive device for neonatal jaundice detection	Provide a non-intrusive solution for early detection of neonatal jaundice	Limited discussion on device accuracy and reliability in real-world clinical settings
[27]	Present a methodology for categorizing mental functioning using wavelets and partial correlation	Introduce a novel methodology for the evaluation of mental function using advanced statistical techniques	There is a lack of discussion on the applicability to diverse populations and clinical settings
[28]	Propose a wearable ECG monitoring system with IoT methods	Offer a novel approach to ECG monitoring for smart healthcare	Limited discussion of the system's battery life, data security, and integration with existing healthcare infrastructure
[29]	Analyze the variability in therapeutic movements using wearable inertial sensors	Provide information on the analysis of the variability of therapeutic movements using wearable sensors	There is a lack of discussion on the accuracy and reliability of wearable sensors for capturing therapeutic movements
[30]	Examine generic intellectual tasks in medical Cyber-Physical-Human Systems	Present an innovative framework for modeling medical guidance systems	Limited discussion of the practical implementation and scalability of the proposed framework

3. Problem statements

The SHS is a contemporary Cyber-Physical System (CPS) that consistently gathers data from the IoMT sensor network linked to the human body. Then it processes this data to make necessary control decisions and

activates Implantable Medical Devices (IMDs) for immediate medication and treatment. Presently, healthcare facilities have become more efficient, readily available, and tailored to individual needs due to the advances made by the SHS in illness diagnosis tools, patient treatment, and healthcare technologies. Consequently, this has resulted in an improvement in the overall quality of life [31]. Nevertheless, an SHS requires analyzing a substantial amount of past data to detect abnormal sensor readings. The healthcare and drug data are abundant. They may be used to uncover complex relationships between several essential indicators of the human body for precise and accurate categorization of diseases. To speed up processing, an SHS incorporates the notion of IoMT with big data, cloud computing, and Artificial Intelligence (AI).

Due to the emergence of SHS, smart medical devices are now vulnerable to several attack vectors, making them prone to possible security risks. The incidence of cyberattacks targeting the healthcare sector is seeing a significant and rapid increase [31]. SHS devices, also known as IMDs, often include vulnerabilities that present substantial risks [32]. A recent survey shows that 53% of healthcare companies experienced cyber attacks between October 2018 and October 2019 [33]. The most prevalent cyberattacks in healthcare systems are hardware Trojans [34], malware such as Medjack [35], Sybil attacks using hijacked IoMT [36] or a single rogue node [37], DoS attacks [38], and Man-In-The-Middle (MITM) attacks [39]. Within the last 20 months, about 20% of medical equipment manufacturers have faced ransomware or malware attacks [40,41]. Therefore, it is crucial to thoroughly examine the weaknesses of a solar home system before its implementation.

3.1 System model

The SHS depicts an advanced network where data from IoMT sensors, integrated into medical equipment and linked to the human body, are consistently gathered. The data serves as the basis for well-informed control choices in the system, allowing prompt reactions and interventions by activating IMDs. The CPS is an integrated ecosystem where medical equipment and sensors interact with data processing and Decision Making (DM) algorithms to improve healthcare delivery. An essential feature of the SHS is its ability to analyze past data to discover anomalous sensor readings and detect future health problems. The technology uses vast healthcare and drug-related data to reveal intricate connections among different physiological indications, aiding in the precise illness classification and tailored treatment strategies. The data analysis process is crucial for SHS to provide customized healthcare solutions that meet the specific requirements of each

patient, thus improving overall healthcare efficiency, accessibility and quality of life. The SHS incorporates many state-of-the-art technologies to effectively manage the large quantities of data produced by IoMT sensors and guarantee prompt and precise DM. These technologies encompass big data analytics, which facilitates efficient processing and extraction of insights from large datasets; cloud computing, which offers scalable and on-demand access to computational resources; and AI, which drives advanced algorithms for data analysis, prediction, and DM. The combination of these technologies speeds up data processing, increases the accuracy of diagnoses, and increases treatment results within the SHS framework.

However, the SHS faces substantial security obstacles, mainly due to the increasing occurrence of cyberattacks aimed at healthcare systems. Intelligent medical devices inside the SHS, such as IMDs, are susceptible to many attack methods, including hardware Trojans, malware, DoS attacks, and MITM attacks. The frequency and complexity of these cyberattacks highlight the crucial significance of conducting a comprehensive assessment of SHS's vulnerabilities before its implementation and establishing strong security measures to protect patient data, privacy, and safety. The Smart Healthcare System is a sophisticated and integrated ecosystem that utilizes IoMT, data analytics, cloud computing, and AI to transform healthcare delivery. To ensure the SHS's dependability, integrity, and trustworthiness of the SHS, it is crucial to handle security concerns successfully. This is necessary to fully use its potential to improve patient outcomes and quality of care while being resilient against changing cyber threats.

3.2 Design of the system model

The system model for the SHS is designed to meet the intricate demands of modern healthcare delivery effectively. The system model is based on a complex sensor network architecture that includes IoMT devices strategically integrated into medical equipment and wearable devices. Sensors collect a large amount of data on patient vital signs, health characteristics, and environmental elements. These data are used to make informed decisions and provide individualized healthcare care. After obtaining the data, the system model utilizes sophisticated data processing and analysis methods to derive significant insights. Real-time processing of sensor data allows the detection of patterns, anomalies, and trends indicative of health issues or possible threats. ML methods, such as deep learning and predictive analytics, are

crucial for quickly and reliably evaluating large volumes of data. Using these algorithms, the SHS can anticipate patient outcomes, suggest treatment procedures, and improve healthcare delivery by considering unique patient profiles and clinical recommendations. The system model relies on a DM framework that interprets examined data and creates suitable responses.

The SHS uses advanced algorithms to assess patient conditions, provide customized treatment plans, and prompt urgent actions. The DM process in healthcare is guided by a comprehensive awareness of the patient's medical history, evaluations of potential hazards, and evaluations of treatment effectiveness. This allows healthcare professionals to maximize patient outcomes while reducing risks and efficiently using resources. The system model effortlessly incorporates cloud computing infrastructure to meet its computational and storage needs. Cloud services provide flexible and expandable resources to store, process, and deploy ML models. This connection improves the SHS's ability to adapt, be versatile, and handle increased demands quickly. It also makes it easier for healthcare professionals to access and work together from a distance.

Additionally, rigorous security and privacy protocols are in place to protect sensitive healthcare data from unauthorized access, manipulation, or breaches. Robust encryption methods, strict access restrictions, and reliable authentication systems guarantee the protection of patient information and adherence to regulatory standards. Interoperability standards are essential in the architecture of the system model as they provide smooth communication and integration with current healthcare IT systems and medical equipment. Compliance with HL7 and FHIR guarantees compatibility and interoperability between various healthcare systems, Electronic Health Records (EHRs), and medical device interfaces. In addition, the system model places a high importance on user experience by providing user-friendly interfaces designed to meet the requirements of healthcare professionals, patients, and caregivers. Intuitive dashboards, mobile apps, and visualization tools provide convenient access to pertinent health data, practical insights, and DM aids, improving acceptance and usefulness across various user demographics. Ultimately, the design of the Smart Healthcare System embodies a comprehensive and unified strategy to transform healthcare delivery. SHS aspires to better patient outcomes, improve care delivery efficiency, and encourage customized and proactive healthcare management by integrating sophisticated technology, strong security measures, interoperability standards, and user-centric design concepts.

4. Proposed scheme

A comprehensive and multifaceted strategy will be needed to solve privacy, security, and trust management problems in smart healthcare systems based on ML and IoT. Fig. 1 displays the proposed system architecture, including techniques and solutions to alleviate the mentioned difficulties. Table 2 represents the notations and description used in this chapter.

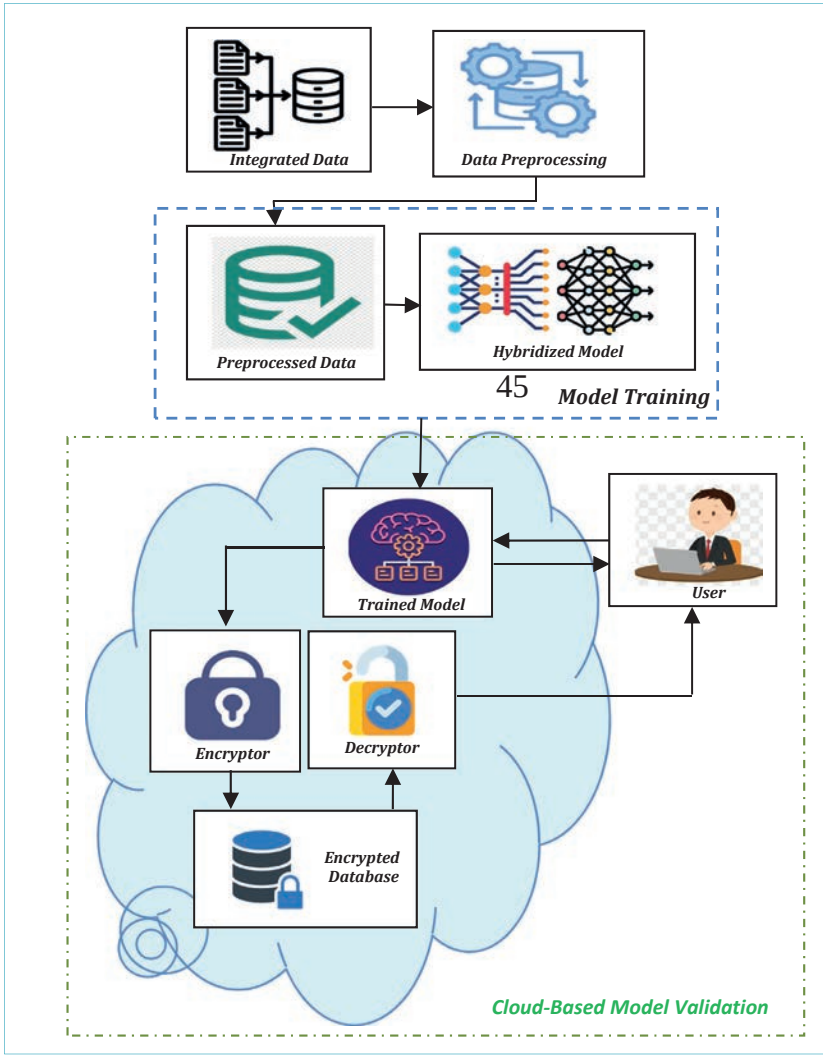


Fig. 1 The proposed system architecture

Table 2 Notations and their description.

Notations	Description	Notations	Description
X	Input sequences (sensor data from IoT devices)	A_t	Context vector
y	Target variable (access level, i.e., authorized or unauthorized)	A	Number of units in the attention mechanism
C	Number of classes in the classification task	W	Weight matrices for input
η	Learning Rate for Optimization	U	Weight matrices for hidden state
T	Number of training epochs	b	Bias vectors
B	Size of mini-batches for training	$X^{(i)}$	A mini-batch of input sequences
$y^{(i)}$	A mini-batch of target variables	c_t	Current cell state
$score(H, S_t, W_a)$	Function to compute attention scores	$softmax(e_t)$	Softmax function to obtain attention weights
$Adam$	Adam optimizer	W_f, U_f, b_f	Forget gate parameters
α_t	Attention weights	W_i, U_i, b_i	Input gate parameters
H	Sequence of hidden states from the LSTM layer	W_c, U_c, b_c	Candidate cell state parameters
S_t	Current hidden state (query)	W_o, U_o, b_o	Output gate parameters
W_a	Weight matrix for the attention mechanism	e_t	Attention scores

4.1 Integrated data

Integrated data is the key component of the strategy to ensure the privacy and security of intelligent healthcare systems built on IoT and ML. In light of the scarcity of publicly accessible and secure medical data, this crucial component keeps user profiles linked to meticulously crafted medical records as seen in Fig. 1.

Integrated data is vital to ensure reliable and legitimate information when training the hybridized ML model for the smart healthcare system. The

system aims to improve healthcare analytics and DM by combining data from credible sources. It is recommended that publicly accessible medical data sources be used to provide more accurate insights and forecasts, resulting in a complete and diversified data set.

This part of the system architecture is crucial to tackle privacy, security, and trust management issues, since it supports the rest of the design. Building efficient ML models requires accurate and diversified medical data, which guarantees that the smart healthcare system runs with the highest standards of accuracy and integrity.

Algorithm 1: Long Short-Term Memory-Attention Mechanism (LSTM-AM) for Smart Healthcare Systems

Input: X, y, A, C, η, T, B
Output: Trained LSTM-AM

1. Start
2. From t=1 *to* T
3. mini-batches of size B
4. For each mini-batch $\left(X^{(i)}, y^{(i)}\right)$, *where* $i = 1.2, \ldots, \left[\frac{N}{B}\right]$
5. LSTM layer given the input sequence $X^{(i)}$
6. Apply *AM*
7. Output probabilities using the output layer
8. Binary cross-entropy loss between the predicted probabilities and the true label $y^{(i)}$
9. Backpropagation and the *Adam*
10. Return Trained *LSTM-AM*
11. End

Algorithm 2: LSTM Algorithm for Smart Healthcare Systems

Input: X, h_t-1, c_t-1, W, U, b, t
Output: h_t, c_t

1. Start
2. $f_t = \sigma(W_f.X + U_f.h_{t-1} + b_f)$
3. $i_t = \sigma(W_i.X + U_i.h_{t-1} + b_i)$
4. $\widetilde{c_t} = \tanh(W_c.X + U_c.h_{t-1} + b_c$
5. $c_t = f_t.c_{t-1} + i_t.\widetilde{c_t}$
6. $o_t = \sigma(W_0.X + U_o.h_{t-1} + b_o)$
7. $h_t = o_t.\tanh(c_t)$
8. Return h_t, c_t
9. End

Algorithm 3: AM Algorithm for Smart Healthcare Systems

Input: H, S_t, W_a, t
Output: A_t

1. Start
2. $e_t = score\ (H, S_t, W_a)$
3. $\alpha_t = softmax(e_t)$
4. $A_t = \sum_{i=1}^{T} \alpha_t$, i H_i
5. Return A_t
6. End

4.2 Data preprocessing

The subsequent pivotal stage in the suggested system architecture for the security, privacy, and trust management of IoT and ML-based SHSs is data preprocessing. This crucial element is precisely engineered to enhance and process integrated medical data obtained from various sources, guaranteeing its suitability for further studies and model creation.

Data preprocessing encompasses a thorough sequence of actions designed to improve the overall quality and usefulness of the integrated medical data. The phases include performing data cleaning, normalization, and transformation procedures to handle any inconsistencies, outliers, or abnormalities in the dataset. By standardizing the data and resolving any possible difficulties, data preprocessing enhances the reliability and precision of ML model training and assessment.

The efficacy of the overall intelligent healthcare system is highly dependent on the integrity of the preprocessed data. Data preprocessing is crucial for assuring the dependability, precision, and confidentiality of the combined medical data, supporting the system's overarching goals of security, privacy, and trust management. The result of this step is the Preprocessed Data repository, as seen in Fig. 1.

4.3 Model design and training

The proposed system architecture for Security, Privacy, and Trust Management in IoT and ML-based SHSs incorporates an essential advancement in the Model Design and Training phase. This advancement involves integrating LSTM-AM. This novel and strategic fusion aims to use the distinct capabilities of LSTM-AM to amplify the intelligence and efficiency of the hybridized ML model.

The integration of LSTM, a sophisticated iteration of Recurrent Neural Network (RNN), provides a strong structure for collecting time-based relationships and maintaining the overall meaning within sequential healthcare data. From a mathematical perspective, LSTM incorporates updating and gating methods using Eq. (1), which outputs the forget gate, f_t at time step t.

$$f_t = \sigma\left(W_f.[h_{t-1}, x_t] + b_f\right) \tag{1}$$

where σ is the sigmoid activation function, W_f is the weight matrix for the forget gate, $h_{\{t-1\}}$ is the hidden state at the previous time step $(t-1)$, x_t is the input at current time step t, and b_f is the bias for the forget gate.

To compute the output of the input gate i_t at time step t, Eq. (2) is used.

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \tag{2}$$

where i_t is the input gate output at time step t, W_i is the weight matrix for the input gate, x_t is the input at current t, and b_i is the bias for the input gate.

The output of the output gate o_t at t is computed using Eq. (3).

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \tag{3}$$

where o_t is the output gate output at time step t, W_o is the weight matrix for the output gate, x_t is the input at current time step t, and b_o is the bias for the output gate.

Eq. (4) updates the cell state at a given time step.

$$c_t = f_t.c_{t-1} + i_t.\,tanh\left(W_c.[h_{t-1}, x_t] + b_c\right) \tag{4}$$

where c_t is the cell state at time step t, f_t is the forget gate output at time step t, $c_{\{t-1\}}$ is the cell state at the previous time step $t-1$, i_t is the input gate output at time step t, *tanh* is the hyperbolic tangent activation function, W_c is the weight matrix for the cell state, and b_c is the bias for the cell state.

Eq. (5) computes the hidden state/output h_t at time step t, determining what information from the cell state c_t should be output, modulated by the output gate o_t, and it is computed using a hyperbolic tangent activation function tanh.

$$h_t = o_t.\tanh(c_t) \tag{5}$$

In addition to LSTM, the AM enhances the model's capacity to identify pertinent information in input sequences. Eq. (6) computes the AM score between the query and key vectors, indicating their similarity or relevance.

$$e_{ti} = \text{score}(query_t, key_i) \tag{6}$$

where $e_{\{ti\}}$ is the score of the AM between the query $text\{query\}_t$ and key $text\{key\}_i$ at time step t.

$text\{score\}(text\{query\}_t, text\{key\}_i)$ = Scoring function that computes the similarity or relevance between the query and key.

Eq. (7) calculates the attention weight, $\alpha_{\{ti\}}$ for each key vector at a given time step, normalizing the scores using the softmax function to represent the importance of each key with the query.

$$\alpha_{ti} = \frac{\exp(e_{ti})}{\Sigma_{j=1}^{T} \exp(e_{tj})} \tag{7}$$

Eq. (8) aggregates the values associated with each key vector, weighted by their corresponding attention weights, to generate the context vector representing the attended information for the query at the current time step.

$$context_t = \Sigma_{i=1}^{T} \alpha_{ti}.value_i \tag{8}$$

where $text\{context\}_t$ is the context vector at t, representing the weighted sum of values and the weights are determined by attention weights $alpha_{ti}$.

The fusion of LSTM-AM is achieved by combining them in a weighted manner. The final hidden state, h_t, is determined by inserting attention weights into the LSTM output, as shown in Eq. (9).

$$h_t^* = \alpha_{t1}.h_1 + \alpha_{t2}.h_2 + \ldots + \alpha_{tT}.h_T \tag{9}$$

where h_t^* represents the output or context vector at t, which is a weighted sum of hidden states h_i and i ranges from 1 to T. α_{ti} represents the attention weight corresponding to the hidden state h_i at t, indicating the importance or relevance of each hidden state in contributing to the context vector h_t^*. h_i represents the hidden state at time step i, where i ranges from 1 to T.

The integration of LSTM-AM embodies a collaborative strategy, amalgamating the advantages of both elements to construct a more potent and flexible model. In addition to enhancing performance, maintaining privacy is of utmost importance. The model incorporates privacy-preserving methodologies to ensure valuable insights are derived from patient data while upholding individual privacy following rigorous healthcare data security protocols.

This advanced model is a state-of-the-art solution in smart healthcare. It is better skilled at comprehending and forecasting intricate temporal connections among the data sequences. This integration provides a strong

basis for advanced analytics and DM by effectively managing the intricacies of Model Design and Training. It prioritizes security, privacy, and trust management. This phase results in a highly skilled model prepared for deployment on the cloud.

4.4 Cloud-based model validation

Within the framework of system design for Security, Privacy, and Trust Management in IoT and ML-based SHSs, the cloud-based model validation phase plays a vital role in upholding the integrity and security of medical information. This section provides an overview of the procedures for confirming data accuracy and implementing steps to protect sensitive information and authenticate information requests. Utilizing Flask, a Python web framework, our ML model is deployed to create a reliable Application Programming Interface (API) that effectively communicates with the cloud server, enabling efficient management of information requests. The medical data saved in the cloud is subjected to encryption to enhance its security and privacy, as seen in Fig. 1. An exclusive module for encryption and decryption guarantees the confidentiality of medical information at all stages of its existence.

The phase also includes the integration of authentication and authorization mechanisms. Upon receiving a request for medical information, the deployed model performs comprehensive authentication checks to confirm the authenticity of the requester. Moreover, the model evaluates the nature of the requested information and applies permission processes to either grant or refuse access, depending on predetermined criteria acquired by the trained deep learning model. After the request is successfully authenticated and authorized, it is sent to the cloud server. The server, equipped with solid security measures, handles the request and creates the answer. A specialized decryptor module is used to ensure the privacy of the sent data. This module performs decryption on the server's response before delivering it to the user who started the information request. This guarantees that confidential medical information may only be accessed in its original, comprehensible format by persons who have been granted authorization.

The cloud-based model validation procedure demonstrates a rigorous approach to ensuring the security and validation of access to medical information. The smart healthcare system employs Flask for deployment, encryption for data safety, and a robust authentication and authorization mechanism. This guarantees that only verified and authorized users can access decrypted and precise medical information. This comprehensive

approach not only strengthens security and trust but also corresponds with the overarching principles of the system design, which prioritize security, privacy, and trust management.

5. Performance analysis

The assessment of hybridized deep learning models is included in the part focused on "Security, Privacy, and Trust Management of IoT and ML-based SHS". This part thoroughly examines the performance of the generated model using a wide range of necessary performance measures. The specified measures, including accuracy, precision, recall, and F1 score, have been carefully chosen to evaluate the system's capability to handle various prediction tasks. These metrics assess the system's ability to protect, keep private, and establish trust in healthcare data in IoT and ML. They provide a detailed assessment of how well the hybrid models work in this important context. This thorough study offers a solid basis for assessing and improving the overall performance of the integrated system within the identified areas.

5.1 Experimental environment

To comprehensively assess the hybridized deep learning model created in this research project for "Security, Privacy, and Trust Management of IoT and ML-based SHS," a detailed experimental setup was meticulously devised. The arrangement of the experimental design is essential for guaranteeing the dependability and replicability of the acquired findings.

The hardware infrastructure used for the studies was crucial in attaining the required results. A high-performance computing system was used to meet the computational requirements of the constructed deep learning (LSTM-AM) model. The system had two Intel Xeon processors, each with seven cores and a clock speed of 2.5 GHz. It also included 16 GB of DDR4 RAM and a high-speed SSD storage array with a capacity of 250 GB. The robust hardware setup guaranteed excellent performance and quick response times during the extended trial phase. The presence of multiple processors enabled parallel processing, which accelerated the training and inference of models. Additionally, the generous amount of memory and high-speed storage supported the rapid retrieval of big datasets, which is crucial for the efficiency of deep learning activities. The meticulous selection of this hardware configuration enhanced the dependability and precision of the experimental findings, enabling a thorough evaluation of the hybrid models'

effectiveness in the designated areas of security, privacy, and trust management within the framework of IoT and ML-based SHSs.

The selection of software frameworks and libraries substantially impacted the development and execution of the deep learning model produced in this study. This research model's execution included the selection and use of TensorFlow and Keras, in addition to the Visual Studio Code (VS Code) Integrated Development Environment. The Python programming language used pandas for data management, Matplotlib for dynamic display, and numpy arrays for fast numerical calculations, all crucial elements in the experimental setting.

TensorFlow, known for its capacity to scale and be ready for production, offered a strong basis for developing and deploying models. Because of its intuitive interface and seamless integration with TensorFlow, Keras improved the efficacy of testing and the development of model prototypes. Matplotlib's dynamic display features enabled in-depth investigation of model performance, while pandas helped smooth data handling and preparation operations.

The efficiency of computational models was enhanced by using numpy arrays, which facilitated numerical data processing. Using the VS Code IDE, TensorFlow, Keras, pandas, matplotlib, numpy arrays, and the Python programming language provided a well-rounded and efficient method for achieving the study objective. Utilizing the advantages of each tool enhanced the execution of the hybridized deep learning model, guaranteeing its efficacy and conformance with established research standards. Implementing this strategic software selection significantly improved the performance of the models, namely in the domain of forecasting medical information access control.

5.2 Dataset description

To train the deep learning model in this study, a dataset of 5000 simulated records was created, as there were no publicly accessible medical user profiles. This dataset is essential for building and assessing a specialized access control system for medical information. The dataset includes several fields specifically chosen to simulate the intricate and varied user responsibilities within a healthcare setting, as shown in Table 3.

1. **Access Levels:** Determine the access rights assigned to each user position, establishing the scope of their authority inside the medical information system

Table 3 User profiles.

Access levels	Authorization policies	Emergency access	User ID	Role	Username	Password
Doctor	Based on the Patient ID	No	U001	Doctor	doc1	jay
Nurse	Based on Symptom Severity	Yes	U002	Nurse	nur1	nur1
Admin	Full Access	No	U003	Admin	adm1	adm1
Technician	Limited Access to Test Results	No	U004	Tech	tec1	Tec1
Researcher	Access to De-identified Data	No	U005	Res	Res	Res
Specialist	Restricted Access to Critical Cases	Yes	U006	Spec	Spec	Spec
Paramedic	Emergency Patient Data Access	Yes	U007	Para	Para	Para
Analyst	Access to Statistical Analysis	No	U008	Ana	Ana	Ana
Support Staff	Limited Access to Administrative Support	No	U009	Sup	Sup	Sup
Auditor	Reviewing Access Logs	No	U010	Aud	Aud	Aud

2. **Authorization Policies:** Establishes the guidelines that dictate access for each position, creating a structure for making decisions based on patient identification, symptom intensity, or other pertinent considerations.
3. **Emergency Access:** Flags indicate whether a user role is allowed emergency access rights, enabling prompt access to vital patient data under urgent circumstances.
4. **User ID:** An exclusive identification issued to each simulated user in the collection.

5. **Position:** Specifies the assigned position or job title for each user, outlining their duties and level of authorization
6. **Username:** Each user is assigned a username, which plays a crucial role in verifying their identity throughout system interactions.
7. **Password**: The exclusive code linked to each username, ensuring authorized entry into the medical information system.

5.3 Results and discussion

Based on the study, the experimental results demonstrated impressive performance outcomes. The system's accuracy rate, which represents the total validity of its predictions, reached an incredible 99.06%. The system's precision in the sensitive healthcare area, which measures its ability to minimize false positives, achieved an impressive level of 98.14%. Similarly, recall, which measures the power of the system to identify positive cases in the context of healthcare security accurately, demonstrated strong performance at a rate of 99.06%. In addition, the F1 score, which considers both accuracy and recall, attained an impressive score of 99.00%. The results emphasize the system's efficiency in producing precise predictions, with high accuracy, recall, and overall performance in the intricate field of "Security, Privacy, and Trust Management of IoT and ML-based SHSs". Fig. 2 presents a graphical

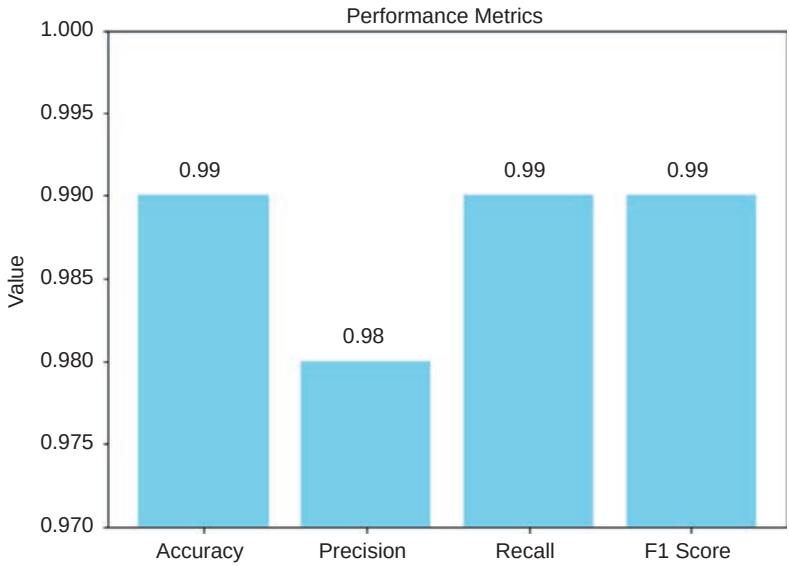


Fig. 2 Performance metrics scores chart.

depiction of the scores for the model's performance indicators, providing a more lucid explanation.

The visual depiction in Fig. 2 vividly demonstrates the model's performance measures, offering a brief overview of its efficacy. The metrics provided include accuracy, precision, recall, and F1 score. An expedited chart analysis facilitates a straightforward understanding of the model's performance across these significant metrics. This visual representation is a helpful instrument, enabling a fast evaluation and comparison of many facets of the model's performance. It enhances the comprehension of its strengths and identifies areas that might be improved. The study used the Receiver Operating Characteristic (ROC) curve to thoroughly analyze the model's performance, as seen in Fig. 3.

The ROC curve, seen in Fig. 3, offers a comprehensive depiction of the predictive performance of the hybridized deep learning model, such as the one generated in this study. The ROC curve illustrates the relationship between the True Positive Rate (Sensitivity) and the False Positive Rate (1—Specificity) at different threshold values. It balances accurately detecting positive examples and wrongly categorizing negative ones. A more excellent value for the area under the receiver operating characteristic curve (AUC)

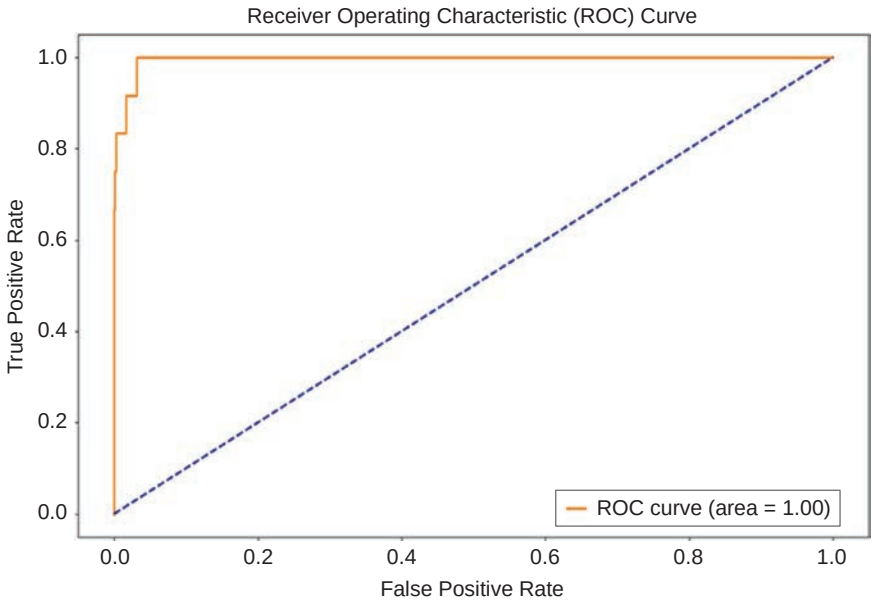


Fig. 3 ROC curve.

signifies enhanced model performance, where a perfect classifier would have an AUC of 1. Within this framework, achieving a ROC area of 100% indicates the model's remarkable capacity to differentiate between genuine positive and false positive occurrences accurately. This provides vital evidence of its faultless efficacy in identifying fraudulent users or intrusions. The visual depiction facilitates comprehension of the model's sensitivity and specificity at various decision thresholds, enhancing a thorough assessment of its classification performance.

5.3.1 Training and validation loss

This research computed a graphical representation of the training and validation loss to analyze the evaluation of the LSTM-AM model developed for Security, Privacy, and Trust Management of IoT and ML-based SHSs further.

The graph in Fig. 4 provides a comprehensive analysis of the performance assessment of the LSTM-AM model, which is specially tailored for the Security, Privacy, and Trust Management of IoT and ML-based SHSs. The graphic especially illustrates the patterns in training and validation loss during the model's training procedure. Within this framework, the training loss denotes the discrepancy experienced by the model as it learns

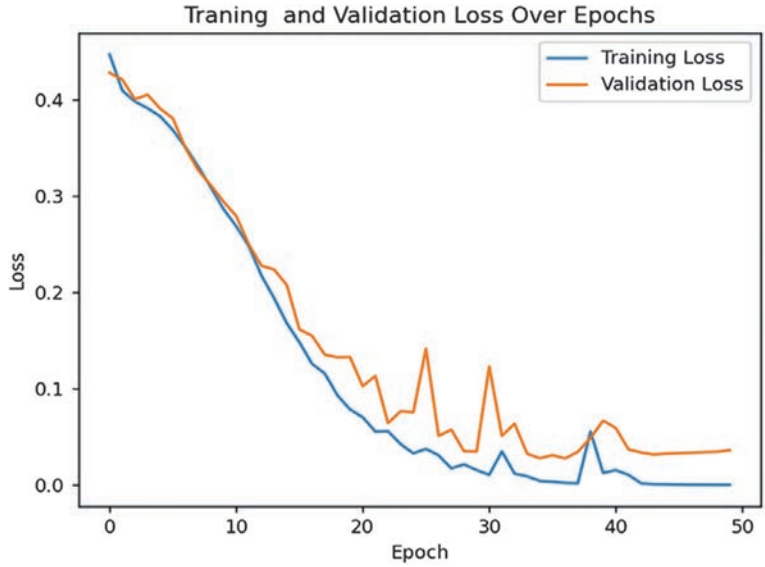


Fig. 4 Training and validation loss.

from the training dataset. In contrast, the validation loss indicates the model's effectiveness on a separate data set not used during training.

An analysis of this plot provides vital insights into the model's learning capabilities from the training data and its capacity to generalize to unfamiliar data, which is crucial for accurately detecting malevolent users. The ideal outcome is to achieve convergence between the training and validation loss, which indicates a well-learned model that is neither overfitting nor underfitting. Minor discrepancies or discontinuities between the two curves indicate specific areas where the model's architecture might be further refined or adjusted to tackle possible problems such as overfitting or inadequate model training.

5.3.2 Training and validation accuracy

As part of the assessment process, we attempted to compute and graphically depict the correctness of the model for both the training and validation data. The visual representation that is obtained is seen in Fig. 5.

Fig. 5 is an assessment chart that shows the hybridized LSTM-AM model that was trained and validated to identify fraudulent access to medical information. The chart gives a complete view of the evaluation. This figure shows how the model's accuracy scores changed while it was being trained

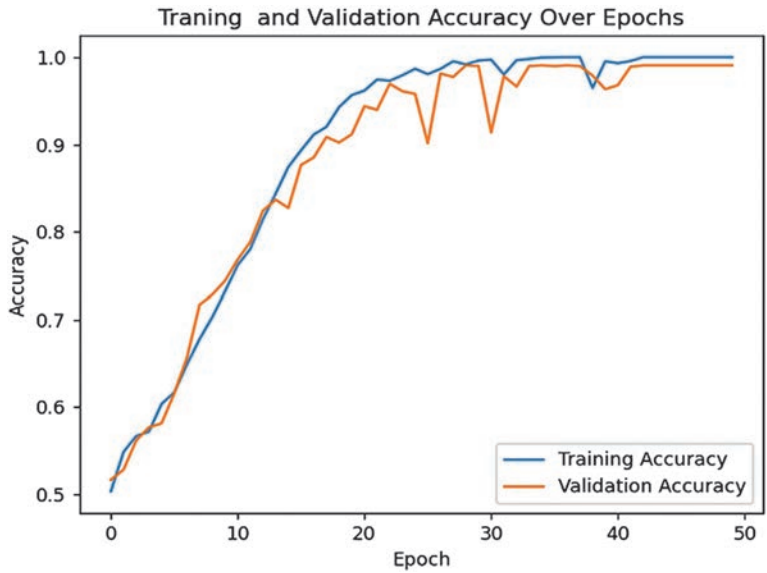


Fig. 5 Training and validation accuracy.

and how it performed on a separate validation dataset. The training accuracy measures the model's predictive power on the training data, and the validation accuracy evaluates its generalizability to new, unseen data.

This figure reveals trends and oscillations in accuracy as the model's learning dynamics pertain to the detection of fraudulent access to medical information. Carefully examining it may evaluate the model's learning dynamics as they pertain to the detection of fraudulent access to medical information. The ideal situation would be to converge training and validation accuracy, meaning the model learned well without getting too hung up on the training data. Overfitting and insufficient model training are possible causes of a diverging or significantly different curve.

These outcomes demonstrate our system's efficacy in producing correct predictions and highlight its excellent performance, recall, and accuracy. The "Security, Privacy, and Trust Management of IoT and ML-based SHSs" visually depicts the integration of IoT and ML. The study highlights the positive outcomes and implications for improving the security and privacy of healthcare data in the smart healthcare domain. The research conducted by Pandey and Prabha [42] employs a Support Vector Machine (SVM) model and achieves an accuracy rate of 86.0%. The SVM is a kind of supervised learning technique that is often used for classification problems. It effectively handles both linear and non-linearly separable data by identifying the ideal hyperplane that best separates the classes. In addition, Balakrishnan et al. [43] use a DT model that achieves a 95.9% accuracy rate. DTs are transparent models that generate predictions by applying a sequence of if-else decision rules. These models are especially well-suited for jobs that need a thorough knowledge of the DM process since they provide transparent insights into how the model reaches its predictions.

Additionally, Khan et al. [44] use an Artificial Neural Network (ANN) and achieve a high accuracy rate of 91.8%. An ANN is a kind of ML model that draws inspiration from the complex neural networks seen in the human brain. The system comprises linked nodes, also known as neurons, that are arranged in layers. It can learn intricate patterns from data. ANN is renowned for its adaptability and capacity to process complex, non-linear connections within datasets effectively. In addition, Munnangi et al. [45] propose a Moran Autocorrelation and Regression-based Elman Recurrent Neural Network (MAR-ERNN), which achieves a high accuracy of 95.0%. This model integrates spatial autocorrelation information using the Moran coefficient and employs a recurrent neural network architecture

(specifically Elman) to capture temporal correlations in the data. Recurrent neural networks are highly suitable for analyzing sequential data, making them very successful in applications such as predicting time series and interpreting spoken language. Finally, the model suggested in the comparison analysis table utilizes LSTM networks and achieves the most remarkable accuracy rate of 99.1%. LSTM is a specific kind of recurrent neural network structure that is specifically developed to tackle the issue of the vanishing gradient problem. This unique architecture enables LSTM to accurately capture and represent long-term relationships and dependencies in sequential data. It is very efficient at tasks that require the comprehension and retention of long-term patterns, such as voice recognition, language translation, and sentiment analysis.

Upon comparing the outcomes of the suggested LSTM model with the five preexisting models, it is clear that the LSTM model surpasses all other models in terms of accuracy, obtaining an accuracy rate of 99.1%, as seen in Fig. 6. The exceptional performance might be ascribed to the LSTM's capacity to apprehend and preserve long-term connections in sequential data, which may be crucial for the particular job. The DT model has robust performance, achieving an accuracy of 95.9%. In contrast, SVM, ANN, and MAR-ERNN get accuracies ranging from 86.0% to 95.0%. To summarize, the comparative analysis in Table 4 showcases the efficacy of several ML-based methods in tackling the problem, with the suggested LSTM model emerging as the most precise. Every model has unique advantages

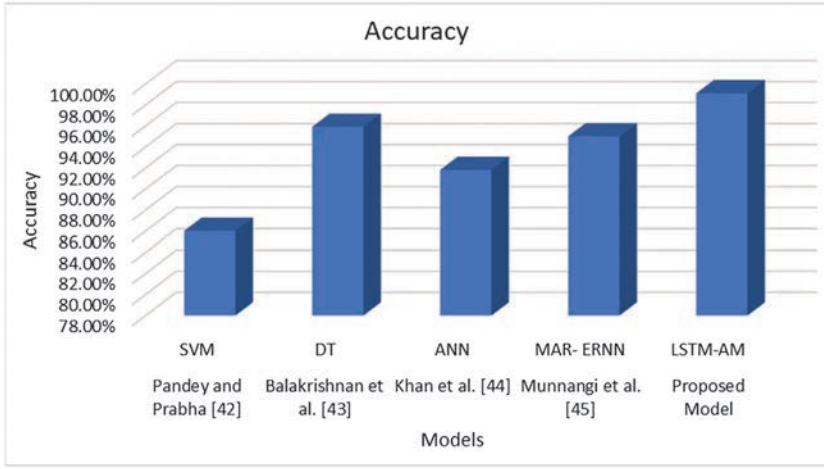


Fig. 6 Comparative analysis with existing systems.

Table 4 Comparative analysis of the proposed scheme and existing schemes.

Scheme	Model	Accuracy (%)
Pandey and Prabha [42]	SVM	86.0
Balakrishnan et al. [43]	DT	95.9
Khan et al. [44]	ANN	91.8
Munnangi et al. [45]	MAR-ERNN	95.0
Proposed Model	LSTM-AM	99.1

and disadvantages, and the selection of a model is contingent upon many criteria, including the characteristics of the data, interpretability needs, and the computing resources at hand.

6. Conclusions

This research scrutinizes integrating IoT and ML in smart healthcare systems, focusing on overcoming security, privacy, and trust challenges essential for safeguarding patient data and system integrity. The proposed advanced system architecture addresses these issues through a comprehensive strategy involving Integrated Data, Data Preprocessing, Model Design and Training, and Cloud-Based Model Validation. Notably, integrating LSTM-AM in the model enhances its ability to capture temporal relationships and focus on relevant data sequences. The model's performance was impressive, with an accuracy of 99.06%, precision of 98.14%, recall of 99.06%, and an F1 score of 99.00%, demonstrating its effectiveness in managing medical information securely and privately. These results were achieved using a synthetic dataset of 5000 records, robust hardware, and sophisticated software frameworks, ensuring comprehensive testing across various scenarios.

This research successfully tackled the complex integration of IoT and ML in smart healthcare systems, setting a standard for ensuring data security and privacy. The developed system architecture and methodology contribute significantly to intelligent healthcare systems, paving the way for future advancements in protecting healthcare information. The study suggests future directions, including advanced ML algorithms, real-world deployment, privacy techniques, cross-domain data integration, user experience,

ethical and legal issues, system robustness, IoT device innovation, healthcare workforce training, and longitudinal studies to comprehensively enhance patient care and system efficiency.

In the future, smart healthcare could focus on advanced ML algorithms, real-world deployment, privacy techniques, cross-domain data integration, user experience, ethical/legal issues, system robustness, IoT device innovation, healthcare workforce training, and longitudinal studies to improve patient care and system efficiency comprehensively.

References

[1] S. Das, S. Namasudra, S. Deb, P.M. Ger, R.G. Crespo, Securing IoT-based smart healthcare systems by using advanced lightweight privacy-preserving authentication scheme, IEEE Internet Things J. 10 (21) (2023) 18486–18494.

[2] S. Namasudra, P. Roy, A new table-based protocol for data accessing in cloud computing, J. Inf. Sci. Eng. 33 (3) (2017) 585–609.

[3] F.A. Adeniyi, J.B. Awotunde, R.O. Ogundokun, P.O. Kolawole, M.K. Abiodun, A.A. Adeniyi, Mobile health application and COVID-19: opportunities and challenges, J. Crit. Rev. 7 (15) (2020) 3481–3488.

[4] J.B. Awotunde, A.E. Adeniyi, R.O. Ogundokun, G.J. Ajamu, P.O. Adebayo, MIoT-based big data analytics architecture, opportunities and challenges for enhanced telemedicine systems, in: Enhanced Telemedicine and e-Health: Advanced IoT Enabled soft Computing Framework, 2021, pp. 199–220.

[5] S. Namasudra, P. Roy, B. Balusamy, P. Vijayakumar, Data accessing based on the popularity value for cloud computing, in: *2017 International Conference on Innovations in Information*, Embedded and Communication Systems (ICIIECS), IEEE, 2017, pp. 1–6.

[6] R.O. Ogundokun, J.B. Awotunde, S. Misra, O.C. Abikoye, O. Folarin, Application of machine learning for ransomware detection in IoT devices, in: Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities, Springer International Publishing, Cham, 2021, pp. 393–420.

[7] S.K. Das, S. Namasudra, A. Kumar, N.R. Moparthi, AESPNet: attention enhanced stacked parallel network to improve automatic diabetic foot ulcer identification, Image Vis. Comput. 138 (2023) 104809.

[8] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. Tsatsoulis, Review of security and privacy for the internet of medical things (IOMT), in: *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE*, 2019, pp. 457–464.

[9] B.A. Alqaralleh, S.N. Mohanty, D. Gupta, A. Khanna, K. Shankar, T. Vaiyapuri, Reliable multi-object tracking model using deep learning and energy efficient wireless multimedia sensor networks, IEEE Access 8 (2020) 213426–213436.

[10] R.O. Ogundokun, J.B. Awotunde, E.A. Adeniyi, F.E. Ayo, Crypto-Stegno based model for securing medical information on IOMT platform, Multimed. Tools Appl. 80 (2021) 31705–31727.

[11] T. Vaiyapuri, V.S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, K. Shankar, A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing, Wirel. Pers. Commun. (2021) 1–24.

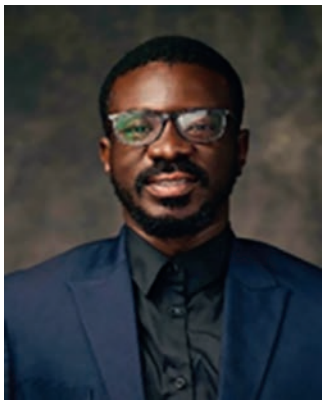
[12] M.K. Abiodun, J.B. Awotunde, R.O. Ogundokun, E.A. Adeniyi, M.O. Arowolo, Security and information assurance for IoT-based big data, in: *Artificial Intelligence for*

Cyber Security: Methods, Issues and Possible Horizons or Opportunities, Springer International Publishing, Cham, 2021, pp. 189–211.
[13] R.O. Ogundokun, R. Maskeliūnas, S. Misra, R. Damasevicius, A novel deep transfer learning approach based on depth-wise separable CNN for human posture detection, Information 13 (11) (2022) 520.
[14] C. Stamate, G.D. Magoulas, S. Küppers, E. Nomikou, I. Daskalopoulos, M.U. Luchini, T. Moussouri, G. Roussos, Deep learning Parkinson's from smartphone data, in: 2017 IEEE International Conference on Pervasive Computing and Communications, IEEE, 2017, pp. 31–40.
[15] G. Lee, K. Nho, B. Kang, K.-A. Sohn, D. Kim, Predicting Alzheimer's disease pro gression using multi-modal deep learning approach, Sci. Rep. 9 (2019) 1–12.
[16] M.O. Arowolo, R.O. Ogundokun, S. Misra, B.D. Agboola, B. Gupta, Machine learning-based IoT system for COVID-19 epidemics, Comput. Secur. 105 (4) (2023) 831–847.
[17] S.S. Rani, J.A. Alzubi, S. Lakshmanaprabu, D. Gupta, R. Manikandan, Optimal users based secure data transmission on the internet ohealthcare things (IOHT) with light-weight block ciphers, Multimed. Tools Appl. 79 (2019) 35405–35424.
[18] A. Alabdulkarim, M. Al-Rodhaan, T. Ma, Y. Tian, Ppsdt: a novel privacy-preserving single decision tree algorithm for clinical decision support systems using IoT devices, Sensors 19 (1) (2019) 142.
[19] R. Boussada, B. Hamdane, M.E. Elhdhili, L.A. Saidane, Privacypreserving aware data transmission for iot-based e-health, Comput. Netw. 162 (2019) 106866.
[20] S. Gull, S.A. Parah, K. Muhammad, Reversible data hiding exploiting huffman encoding with dual images for iomt based healthcare, Comput. Commun. 163 (2020) 134–149.
[21] P. Huang, L. Guo, M. Li, Y. Fang, Practical privacy-preserving ecg-based authentication for iot-based healthcare, IEEE Internet Things J. 6 (5) (2019) 9200–9210.
[22] X. Xu, M. Zhong, J. Wan, M. Yi, T. Gao, Health monitoring and management for manufacturing workers in adverse working conditions, J. Med. Syst. 40 (2016) 1–7.
[23] K. Lin, T. Xu, A novel human body area network for brain diseases analysis, J. Med. Syst. 40 (2016) 1–8.
[24] M.S. Hossain, Patient state recognition system for healthcare using speech and facial expressions, J. Med. Syst. 40 (2016) 1–8.
[25] C.F. Lai, R.H. Hwang, Y.H. Lai, An intelligent body posture analysis model using multi-sensors for long-term physical rehabilitation, J. Med. Syst. 41 (2017) 1–15.
[26] M. Aydın, F. Hardalaç, B. Ural, S. Karap, Neonatal jaundice detection system, J. Med. Syst. 40 (2016) 1–11.
[27] Y. Karaca, Z. Aslan, C. Cattani, D. Galletta, Y. Zhang, Rank determination of mental functions by 1D wavelets and partial correlation, J. Med. Syst. 41 (2017) 1–10.
[28] Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, An IoT-cloud based wearable ECG monitoring system for smart healthcare, J. Med. Syst. 40 (2016) 1–11.
[29] I.H. López-Nava, B. Arnrich, A. Muñoz-Meléndez, A. Güneysu, Variability analysis of therapeutic movements using wearable inertial sensors, J. Med. Syst. 41 (2017) 1–19.
[30] A.Y.Z. Ou, Y. Jiang, P.L. Wu, L. Sha, R.B. Berlin, Preventable medical errors driven modeling of medical best practice guidance systems, J. Med. Syst. 41 (2017) 1–12.
[31] H. Demirkan, A smart healthcare systems framework, IT Prof. 15 (5) (2013) 38–45.
[32] S. Tian, W. Yang, J. Le Grange, P. Wang, W. Huang, Z. Ye, Smart healthcare: making medical care more intelligent, Glob. Health J. 3 (3) (2019) 62–65.
[33] CBS News, Healthcare Industry Saw 63% More Cyberattacks in 2016, 2017. https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/. Accessed: 2020-01-09.

[34] CBS News, How Medical Devices Like Pacemakers and Insulin Pumps Can Be Hacked, 2018. https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/. Accessed: 2020-01-08.
[35] Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses, 2019. https://www.keeper.io/hubfs/PDF/2019%20Keeper%20Report%20V7.pdf.
[36] T. Wehbe, V. Mooney, A. Javaid, O. Inan, A novel physiological features-assisted architecture for rapidly distinguishing health problems from hardware trojan attacks and errors in medical devices, in: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 106–109.
[37] D. Storm, Medjack: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks, 2015. https://www.computerworld.com/article/2932371/medjackhackers-hijacking-medical-devices-to-create-backdoors-in-hospitalnetworks.html. Accessed: 2020-01-08.
[38] A. Almogren, I. Mohiuddin, I.U. Din, H. Al Majed, N. Guizani, FTM-IOMT: Fuzzy-based trust management for preventing sybil attacks in internet of medical things, IEEE Internet Things J. 8 (6) (2020) 4485–4497.
[39] V. Bapuji, D.S. Reddy, Internet of things interoperability using embedded web technologies, Int. J. Pure Appl. Math. 120 (6) (2018) 7321–7331.
[40] J.B. Awotunde, R.G. Jimoh, R.O. Ogundokun, S. Misra, O.C. Abikoye, Big data analytics of IoT-based cloud system framework: Smart healthcare monitoring systems, in: Artificial Intelligence for Cloud and Edge Computing, Springer International Publishing, Cham, 2022, pp. 181–208.
[41] V. Pournaghshband, M. Sarrafzadeh, P. Reiher, Securing legacy mobile medical devices, in: International Conference on Wireless Mobile Communication and Healthcare, Springer, 2012, pp. 163–172.
[42] H. Pandey, S. Prabha, Smart health monitoring system using IOT and machine learning techniques, in: *2020 Sixth International Conference on Bio Signals*, Images, And Instrumentation (ICBSII), IEEE, 2020, pp. 1–4.
[43] S. Balakrishnan, K.S. Kumar, L. Ramanathan, S.K. Muthusundar, IoT for health monitoring system based on machine learning algorithm, Wirel. Pers. Commun. (2022) 1–17.
[44] M.F. Khan, et al., An IoMT-enabled smart healthcare model to monitor elderly people using machine learning technique, Comput. Intell. Neurosci. (2021).
[45] A.K. Munnangi, et al., Survival study on deep learning techniques for IoT enabled smart healthcare system, Health Technol. 13 (2) (2023) 215–228.

About the authors

Dr. Roseline Oluwaseun Ogundokun is a distinguished lecturer in Computer Science at the College of Pure and Applied Sciences, Landmark University, Omu Aran, Kwara State, Nigeria. She holds a Bachelor of Science in Management Information Systems from Covenant University, Ota, and a Master of Science in Computer Science from the University of Ilorin, where she also earned her Ph.D. in computer science. Currently, she is pursuing a second Ph.D. in multimedia engineering at Kaunas University of Technology, Kaunas, Lithuania. Ogundokun's research contributions have garnered significant recognition. According to the SciVal analysis based on SCOPUS-Elsevier data, she is ranked 28th in Nigeria as of June 2023, following previous rankings of 23rd in June 2022, 50th in 2021, and 175th in 2020. She has an impressive publication record with approximately 131 articles indexed in SCOPUS and 171 publications listed in Google Scholar and Web of Science (WoS), collaborating with over 50 coauthors worldwide. Her research interests include computer vision, deep learning, medical imaging, image processing, steganography and cryptography, information security, and artificial intelligence. Ogundokun's honors and awards include the Elsevier Certificate of Recognition as Secretary for SDGs 11—Sustainable Cities and Communities, the Certificate of Excellence for being among the 2021 SCIVAL Top 500 Nigerian Authors on the Scopus platform, and the 2022 Certificate of Excellence for being among the 2022 SCIVAL Top 500 Nigerian Authors on the Scopus platform, both awarded by Landmark University Omu Aran.



Dr. Muhtahir Oluwaseyi Oloyede is a Senior Lecturer at the Department of Information Technology, University of Ilorin where he currently serves as the Head of the Department. His expertise includes Applied Artificial Intelligence, Biometrics, and Wireless Sensor Networks. He has authored several articles in high-impact journals.

Dr. Hakeem Babalola Akande explores the fields of Machine Learning (ML), Network Security, and Artificial Intelligence (AI) in Systems and Networking; he realizes that he is at the vanguard of a technological revolution. In my study of machine learning, a crucial aspect of artificial intelligence, he focus on using algorithms and statistical models to enable systems to improve their performance via experience without explicit programming. This use is very influential in network systems, as he employs machine learning techniques to predict network traffic patterns, detect abnormalities, and optimise complex decision-making procedures. Integrating AI and ML dramatically enhances the effectiveness of Network Security, which is a crucial component in modern networks. By harnessing the power of artificial intelligence, he creates security systems that can analyze vast amounts of network data in real time. This allows me to quickly and accurately detect and neutralize threats, exceeding traditional approaches. These systems can constantly adjust and improve defensive measures by learning from new security issues. Moreover, my use of AI in Systems and Networking facilitates enhanced network administration, proactive maintenance, and enhanced user experiences, owing to intelligent automation and advanced analytics. By integrating artificial intelligence (AI) and machine learning (ML) into network

infrastructures, he contribute to developing knowledgeable, self-regulating, and secure networks capable of predicting and reacting to the ever-changing needs of the digital world.

Julius Olaniyan is a Ph.D. holder in Computer Science from Landmark University, Omu-Aran, specializes in Artificial Intelligence, Machine Translation, Algorithm, and Graph Theory in his research endeavors. His dedication to the field of Artificial Intelligence dates back to 2014. In 2006, he earned his Higher National Diploma in Computer Science from Auchi Polytechnic, Auchi, Edo State, Nigeria. Furthering his academic pursuits, he obtained a Postgraduate Diploma and a Master's Degree in Computer Science from the Federal University of Technology, Akure, Ondo State, Nigeria, in 2012 and 2019, respectively. His educational journey also includes a Bachelor's Degree in Computer Science from Federal University of Oye-Ekiti, Ekiti State, Nigeria, conferred in 2022. He has been active in the software development field since the year 2000, when he completed his National Diploma from the Computer Science department at Auchi Polytechnic, Auchi, Edo State, Nigeria. Proficient in various programming languages such as Visual Basic, Java, Kotlin, C#, Python, PHP, and JavaScript, he has demonstrated his skills by developing desktop, web, and mobile applications for both private and public organizations.

Deborah Olaniyan is a Lecturer, who specializes in research areas encompassing AI-Edu, Computer Vision, Learning Analytics & Assessment, Information Systems & Technology, and Human-Computer Interaction. Her journey in the field of E-learning research began in 2016 during her final year as a Master's student. Her educational background includes a Higher National Diploma in Computer Science from Lagos State Polytechnic, Ikorodu, Nigeria. She continued her academic pursuit with a Postgraduate Degree and a Master's Degree in Management Information Systems (MIS) at the esteemed Covenant University, Ota, Nigeria, achieved in 2015 and 2017, respectively. Furthermore, she holds a BSc in Computer Science from the Federal University of Oye Ekiti, Ekiti State, Nigeria, earned in 2022. Her academic journey reached its pinnacle with the attainment of her highest degree, a Ph.D., from Landmark University, Kwara State, Nigeria. Deborah is characterized as a hardworking, motivated, and enthusiastic individual. In her research domains, she is poised to both contribute to and learn from a diverse range of research backgrounds.

Dr. Chinecherem Umezuruike is an Assistant Professor at Bowen University in Iwo, Osun State. He holds a distinguished academic record and contributes significantly to his field through both teaching and research. His areas of expertise encompass Machine Learning, Internet of Things and Health Informatics. He is actively involved in various scholarly activities and has published numerous articles in reputable academic journals. He is dedicated to advancing knowledge and fostering academic excellence at Bowen University.