A Novel Internet of Things and Cloud Computing-Driven Deep Learning Framework for Disease Prediction and Monitoring

Bo GUO*, Lei NIU

School of Computer and Information Engineering, Fuyang Normal University, Fuyang, 236037, China

***Abstract*—In smart cities, the e-healthcare systems aided by Internet of Things (IoT) technologies play a significant role in proficient health monitoring services. The sensitivity and number of users in health networks highlights the necessity of treating security attacks. In the era of rapid internet connectivity and cloud computing services, patient medical information is most sensitive, and its electronic representation poses privacy and security concerns. Moreover, it is challenging for the traditional classifier to process a massive amount of health data and classify patients' health statuses. To address this matter, this paper presents a novel healthcare model, IoT-CDLDPM, to estimate patients' disease levels using original data and fuzzy entropy extracted from patients' remote locations. IoT-CDLDPM incorporates a deep learning classifier to analyze extensive patient-related data and provides efficient and accurate health status predictions. Furthermore, the proposed model presents the secured storage structure of the individual's health data in cloud servers. To give the authenticity of the health data, two new cryptographic algorithms are presented that encrypt and decrypt the data securely transmitted through the network. A comparison with existing methods reveals that the proposed system significantly reduces computation time, with a recorded time of 0.5 seconds, outperforming DSVS, PP-ESAP, and DRDA by up to 80%. Furthermore, the proposed cryptographic model enhances security levels, achieving a range between 99.4% and 99.8% across multiple experimental setups, surpassing other widely used encryption algorithms such as AES, RSA, and ECC-DH.**

***Keywords*—IoT-driven healthcare; deep learning; fuzzy entropy; secure data storage; cryptography**

I. Introduction

The convergence of cutting-edge technologies has recently led to revolutionary changes in the healthcare sector. Among these, the Internet of Things (IoT) stands out as a pivotal paradigm, transforming health monitoring and management [1, 2]. IoT denotes a network of connected items and sensors communicating seamlessly over the Internet, facilitating real-time data gathering and dissemination [3]. In healthcare, IoT enables the creation of smart environments where medical devices, wearables, and sensors collaborate to gather patient-specific information [4, 5]. This interconnectedness empowers healthcare professionals with timely and comprehensive data, fostering more accurate diagnostics, personalized treatments, and efficient disease management [6].

Cloud computing has become a cornerstone in reshaping healthcare systems infrastructure. The cloud offers a flexible and centralized system for keeping and managing vast healthcare data [7]. It provides the flexibility to access information from anywhere, at any time, facilitating seamless collaboration among healthcare providers and enabling the delivery of telemedicine services [8]. Moreover, the cloud's robust storage capabilities alleviate the burden of data management, ensuring the security and accessibility of patient records [9]. Complementing these advancements, deep learning, a branch of artificial intelligence, has proven instrumental in deciphering intricate patterns within voluminous datasets [10]. Deep learning algorithms recognize complex relationships in healthcare data, making them particularly adept at disease prediction and classification tasks [11, 12]. Leveraging deep learning within the healthcare domain enhances the accuracy of diagnostics and prognostics, leading to the advent of precision medicine [13]. This paper explores the synergistic integration of IoT, cloud computing, and deep learning in designing a novel healthcare monitoring system, addressing the challenges posed by disease prediction and data security in the era of digital health [14].

This paper makes several noteworthy contributions to healthcare monitoring and data security. First, it introduces a novel, robust, and secure storage algorithm designed to maintain the consistency and safety of data stored in cloud databases. Second, the study proposes an innovative deep learning framework to predict health statistics collected via IoT sensors. Third, an encryption scheme is presented to securely protect the stored data, complemented by a corresponding decryption algorithm for accurate data retrieval. Additionally, the paper introduces intelligent fuzzy rules, contributing to effective decision-making based on medical IoT data.

Moreover, this research presents a new formula for ranking patient data, enhancing the prioritization of critical health information. The study also implements spatial and temporal constraints on a Convolutional Neural Network (CNN) classifier, refining its ability to accurately predict patients' health conditions. Finally, the paper systematically conducts various experiments to evaluate the effectiveness of the developed health-tracking approach. Collectively, these contributions advance the current understanding and capabilities in healthcare data security, predictive analytics, and decision-making within the context of IoT-enabled health monitoring systems.

This article is divided into several sections. Section 2 delves into the backgrounds, offering an in-depth exploration of the

contextual foundations relevant to the study. Section 3 elucidates the proposed framework, outlining the intricacies of the developed healthcare monitoring system. Section 4 summarizes the experimental observations, providing a detailed assessment of the system's efficiency in various scenarios. In section 5, the paper concludes by highlighting results, implications, and future research topics.

II. BACKGROUND

Integrating IoT, cloud computing, and deep learning in healthcare requires a thorough understanding of the challenges and opportunities within the rapidly evolving digital health landscape. Table I compares publications highlighting different methods and techniques of enhancing healthcare systems through these technologies. This section offers insight into the existing state of healthcare systems, emphasizing the growing reliance on interconnected devices, the significance of secure data storage, and the pivotal role of advanced data analytics in disease prediction and monitoring.

TABLE I. AN OVERVIEW OF RELATED WORKS

Study	Objective	Key techniques	Performance metrics
[15]	Identify and trace cyber-attack events in IoT networks	Network data flow extraction, PSO for deep learning parameter optimization, PSO-based DNN	Superior performance in detecting and tracing cyber-attacks
[16]	Early detection of thyroid infections	Fog computing, AI, ensemble-based classifier, encryption and decryption	Accuracy, precision, specificity, sensitivity, F1 score
[17]	Remote patient monitoring to reduce hospital visits	IoT, AI, NN configuration optimization, IoT protocols for data transmission	Not specified
[18]	Enhance privacy-preserving healthcare systems	Fog-enabled model, CNN with Bi-LSTM, Medical Entity Recognition, delta sanitizer	Recall, precision, F1-score, utility preservation
[19]	Detection of cardiovascular diseases	IoT, deep learning, BiLSTM for feature extraction, AFO for hyperparameter optimization, FDNN classifier	Accuracy (maximum 93.4%)

In the era of ubiquitous IoT technologies, everyday devices seamlessly connect to the Internet, delivering intelligent functions and on-demand capabilities to users. Despite their lightweight structure and low power consumption, these devices often expose themselves to cyber risks, adversely impacting their functionality within network systems. A significant challenge in securing IoT networks revolves around identifying and tracking sources of cyber-attack events, particularly in the context of obfuscated and encrypted network traffic.

Addressing this challenge, Koroniotis, et al. [15] have developed a novel forensic network methodology known as the Particle Deep Framework (PDF). This framework delineates the phases of digital investigation aimed at detecting and monitoring malicious activities within IoT systems. The PDF introduces three distinctive features: the extraction of data flow patterns and verification of data integrity, tailored explicitly for encrypted networks; the utilization of a Particle Swarm Optimization (PSO) algorithm for the adaptive tuning of deep learning variables; and the design of a Deep Neural Network (DNN) utilizing PSO, designed to identify and monitor anomalies within IoT networks associated with home automation. To assess the efficacy of the presented PDF, evaluations are conducted using UNSW_NB15 and Bot-IoT sources, and comparative analyses are performed using different deep learning algorithms. The test outcomes underscore the superior ability of the PDF in detecting and tracing cyber-attack events compared to alternative strategies.

Various physiological activities are regulated by the thyroid gland, a crucial organ of the endocrine system. These processes include building proteins, energy metabolism, and hormone response. Accurate characterization and reconstruction of the thyroid are essential for detecting thyroid conditions, as alterations in the gland's shape and size indicate potential health issues. Understanding the origins and progression of thyroid diseases is paramount, necessitating focused research in this domain. The intersection of IoT, artificial intelligence, and cloud computing offers immediate computation capabilities with diverse applications in the healthcare sector. Machine learning algorithms are increasingly used in critical decisions. Individuals with thyroid conditions require a reliable and time-sensitive Quality of Service (QoS) framework.

Singh, et al. [16] have innovatively integrated artificial intelligence and fog computing into intelligent healthcare, establishing a reliable mechanism for quickly diagnosing thyroid infections. A novel ensemble-based classifier is introduced for identifying thyroid patients, utilizing UCI datasets, and simulations are conducted using Python programming. In addition to detection accuracy, the proposed framework emphasizes security through authentication and encryption. The effectiveness of the proposed framework is comprehensively assessed for power, RAM, and bandwidth usage. Simultaneously, the potential classifier's effectiveness is evaluated based on F1 score, sensitivity, specificity, precision, and accuracy. The results demonstrate that the developed methodology and classifier significantly outperform traditional methods in addressing thyroid disease detection complexities.

Singh, et al. [17] have developed e-health tools and telemonitoring systems to reduce hospitalizations, particularly in epidemic situations. This initiative leverages artificial intelligence and IoT to tackle these challenges effectively. This research aims to determine the most suitable and efficient configuration of hidden layers and encoding functions for a Neural Network (NN). Subsequently, the information transmitted through IoT networks is elucidated. The NN, an integral project component, scrutinizes information received from sensor data to make informed decisions. The selected condition is subsequently conveyed to the attending medical professional. This innovative tool empowers patients to independently recognize and predict illnesses, aiding healthcare professionals in remote disease detection and analysis.

Significantly, this is achieved without physical hospital visits, enhancing healthcare accessibility and efficiency.

Traditional health systems often struggle to manage vast volumes of biomedical data, leading to cloud-based storage and sharing. However, this approach introduces security challenges, particularly regarding privacy and confidentiality breaches. To address these issues, Moqurrab, et al. [18] have introduced an innovative fog-based data privacy model named "delta sanitizer", leveraging deep learning to enhance healthcare systems. The algorithm developed is built upon a Convolutional Neural Network with Bidirectional Long Short-Term Memory (Bi-LSTM) and is proficient in recognizing health-related entities. Statistical findings indicate that the delta sanitizer model surpasses existing models, achieving a recall of 91.1%, a precision of 92.6%, and an F1-score of 92%. Notably, the sanitization model demonstrates a 28.7% improvement in utility preservation compared to contemporary approaches. This underscores the efficacy of the proposed model in balancing the imperatives of privacy preservation and data utility in biomedical contexts.

Technological advances in the IoT, sensing technologies, and wearables have led to significant enhancements in healthcare quality, shifting from traditional healthcare approaches to continuous monitoring. Sensors attached to biomedical devices capture bio-signals generated by human actions, with the biomedical electrocardiogram (ECG) signal being a standard and non-invasive method for examining and diagnosing cardiovascular diseases (CVDs) rapidly. Given the challenges posed by the increasing number of patients and the diverse ECG signal patterns, computer-assisted automated diagnostic tools play a crucial role in ECG signal classification. In response to this need, Khanna, et al. [19] have introduced an innovative healthcare disease diagnosis model that integrates IoT and deep learning algorithms to analyze biomedical ECG signals. The model's primary objective is CVD detection through deep learning models of ECG signals. Bidirectional Long Short-Term Memory (BiLSTM) enhances the model's ability to extract meaningful feature vectors from ECG signals. The performance of the BiLSTM is further improved by leveraging the Artificial Flora Optimization (AFO) algorithm as a hyperparameter optimizer. A Fuzzy Deep Neural Network (FDNN) classifier assigns appropriate class labels to ECG signals. The model's accuracy is rigorously evaluated using biomedical ECG signals, and the test results confirm its superiority, achieving a maximum accuracy of 93.4%. This underscores the potential of the proposed model in advancing healthcare diagnostics through the fusion of IoT and deep learning technologies.

III. Proposed Framework

Fig. 1 presents a comprehensive overview of the proposed healthcare monitoring system, comprising nine core modules: IoT devices, cloud database, temporal manager, rule base, rule manager, prediction, secure storage, decision manager, and user interface. Patient health data is captured by IoT devices and transmitted to a data collection agent, which stores the information in a cloud-based database. The user interface facilitates data retrieval from this cloud repository, enabling seamless access. Extracted data is then channeled to the decision manager for subsequent processing and secure storage. The latter incorporates a robust security framework comprising encryption, decryption, and key generation components. A novel RSA-based encryption algorithm safeguards data, while the corresponding decryption algorithm ensures data integrity. The efficient key generation algorithm underpins the entire cryptographic process. Encrypted data is persistently stored in the cloud database and can be retrieved upon user request through the user interface, with the decision manager orchestrating the process.

Patient statistics are forwarded to the prediction component for disease level estimation. This module leverages a novel deep learning architecture, the Fuzzy-Temporal Convolutional Neural Network (FTCNN), to accurately determine the severity of diseases. The temporal manager ensures data timeliness, while the spatial manager verifies patient location. The rule manager constructs and finalizes fuzzy rules stored in the rule base for subsequent disease prediction. The decision manager guides rule generation and interprets prediction outcomes, conveying results to physicians and patients. The IoT-CDLDPM framework encompasses three primary components: IoT-based data acquisition, secure data storage, and advanced disease prediction, which are discussed in this section.

Initial patient data is collected from remote locations using IoT devices tailored to specific diseases such as cancer, cardiovascular conditions, and diabetes. These devices employ specialized sensors to capture relevant patient symptoms, including glucose levels, heart rate, and electrocardiogram data. Extracted features are organized into individual patient records, each uniquely identified. The collected data is securely transferred to the cloud database through a coordinated process involving the decision manager, user panel, and data gathering component, with a secure storage component playing a critical role. The data capture component aggregates data and forwards it to the user interface, identifying essential characteristics and passing them to the decision manager for security processing. Subsequently, the decision manager transmits preprocessed data to the storage component for encryption, decryption, and secure cloud storage.

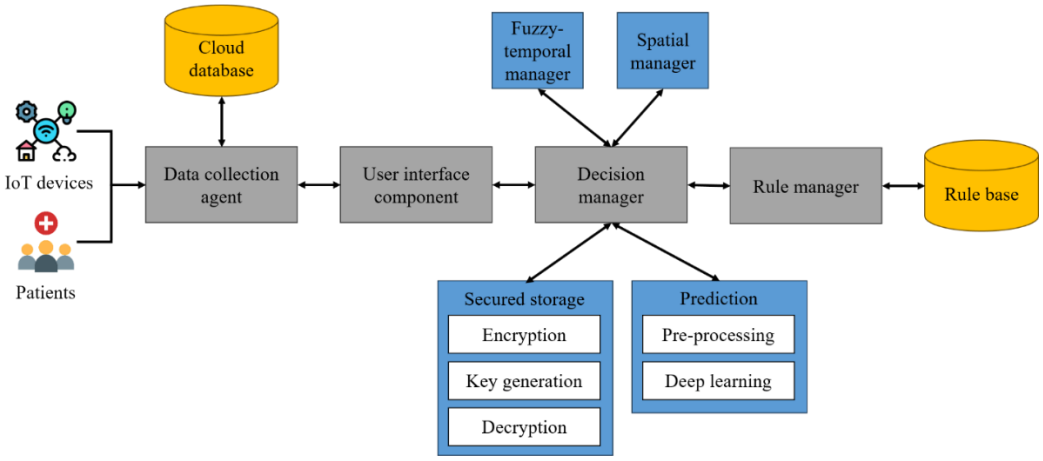

Fig. 1. An overview of the proposed healthcare monitoring system.

The proposed secure storage framework incorporates novel key generation, encryption, and decryption algorithms to safeguard medical and patient data. The initial phase involves key generation using an Elliptic Curve-based Key Generator (ECKG). This algorithm extracts a 4-bit cloud user code, partitioning it into two binary values (*a* and *b*). A prime number (*p*) is selected to define the Galois Field (GFp). Subsequently, the ECKG employs the Diffie-Hellman key exchange protocol to generate public keys P_A and P_B.

An additional layer of protection is introduced through the novel RSA-based Key Generator (RSAKG) to enhance security further. This algorithm derives key pairs (*e* and *d*) from specific points (*q* and *r*) on the elliptic curve. The RSAKGA process involves calculating *n* and *U* and generating public and private keys.

We employ the elliptic curve cryptography-based cyclic encryption procedure (ECC-CEP), which involves two sequential stages. The first stage utilizes elliptic curve-based encryption, while the second employs RSA-based encryption, enhancing the overall security of the process. This comprehensive approach ensures the confidentiality and integrity of the transmitted data.

To complete an entire cryptographic cycle, the suggested elliptic curve cryptography and RSA-enabled multi-decryption scheme are applied to decrypt the original text. This algorithm involves a two-stage process where the first stage utilizes RSA-based decryption, and the second involves ECC-based decryption. Integrating these cryptographic techniques establishes a robust and multilayered security framework for ensuring the privacy and integrity of healthcare data.

The predictive model comprises two principal modules to assess disease severity based on symptoms and patient feedback. The initial module utilizes a deep learning approach to analyze symptom-based severity, evaluate patient feedback textually, and estimate sentiment scores specific to individual diseases to determine their severity level. Subsequently, the model incorporates severity rating features alongside user feedback, allowing for evaluating severity-based ratings and indicating the disease status for specific data instances.

Severity classification relies on the extraction of salient features from patient data. This study proposes an MCST-CNN architecture to accurately determine disease severity and compute patient polarity scores. To refine severity categorization, Latent Dirichlet Allocation (LDA) is employed to cluster extracted severity levels. The MCST-CNN model is a specialized CNN architecture comprising four distinct channels for abnormal, medium, low, and average severity states. Dataset features are mapped to a linear matrix via a lookup function, resulting in a matrix $X \in R^{nk}$. The severity level embedding channel refines severity estimation by incorporating a 45-dimensional severity analyzer vector.

The convolutional layer is instrumental in extracting salient features from medical datasets, reports, and physician notes. By applying filters of varying sizes, this layer effectively identifies crucial attributes for feature and severity level embedding. Given a filter $wt_x \in R^{h \times k}$, where *h* refers to the height of matrix *x* embedded in a particular channel, feature extraction is performed according to Eq. (1) within defined temporal and spatial boundaries. *ATT* denotes an asymmetric curve and *b* represents a bias term. The resulting attribute map, $CH_x \in R^{n-h+1}$, is calculated for a specific time interval (*t1* to *t2*) as outlined in Eq. (2). For severity merging and attribute embedding within the embedding channel, distinct filters $wt_z \in R^{h \times 1}$ are employed to generate attribute maps as described in Eq. (3). This approach enables the generation of diverse feature representations and attributes.

$$CH_i\langle t1, t2, sp\rangle = ATT(wt.x_{i+h} + b) \quad (1)$$

$$CH_x\langle t1, t2, sp\rangle = [CH_1^x, CH_2^x, \dots, CH_{n-h+1}^x] \quad (2)$$

$$CH_z\langle t1, t2, sp\rangle = [CH_1^z, CH_2^z, \dots, CH_{n-h+1}^z] \quad (3)$$

The pooling operation is pivotal in capturing maximum features from input values, typically expressed as shown in Eq. (4). Following this operation, the ultimate attributes are obtained by concatenating the semantically significant attributes using a filter. Typically, this process is denoted as $CH = \underset{x}{CH}^{1} \oplus \underset{z}{CH}^{1}$. Eq. (5) illustrates the resulting final attributes, where the terms *n* and *m* denote distinct thresholds for useful and attribute-specific components, correspondingly.

$$CH_x = MAX(CH_x)\ and\ CH_z = MAX(CH_z) \quad (4)$$

$$CH = \overset{1}{CH}_x \oplus \ldots \oplus \overset{n}{CH}_x \oplus \overset{1}{CH}_z \oplus \ldots \overset{m}{CH}_z \quad (5)$$

Typically, the softmax function is utilized to compute the final attributes. In this research, the extraction of severity levels is framed as a sequential labelling task. The resulting output is represented by Eq. (6), in which O denotes the masking function and $rs \in R^{n+m}$ signifies a sample based on the Bernoulli pattern.

$$0\langle t1, t2, sp\rangle wt.(c\ o\ rs) + b \quad (6)$$

The dataset comprising patient records encompasses a diverse range of attributes associated with severity levels, although variations in the specific attributes are relevant to each severity group. Moreover, the attributes representing severity encompass various types of severity. Hence, it becomes imperative to cluster the pertinent attributes and establish mappings between the extracted severity-related attributes and their respective counterparts. The standard Linear Discriminant Analysis (LDA) method is employed to identify the relevant characteristics from the standardized dataset. Leveraging the LDA method enables segregating specific severity levels into distinct groups. Notably, the LDA method incorporates considerations of spatial and temporal factors, representing an improvement over prior approaches.

Predicting disease severity entails clustering pertinent features and calculating polarity scores for each severity level. Severity level ratings within a rating matrix are determined by computing polarity scores corresponding to severity levels and considering the resulting polarity score. This methodology calculates the rating for each disease severity based on relevant attributes associated with the dataset. The severity level rating is computed using Equation (7), where W_k denotes the word set DS_{ij} linked to severity score a_k, and $SVL(w)$ represents the attribute polarity based on their semantic content.

$$r_{ijk}\langle t1, t2, sp\rangle = \frac{\sum_{w \in W_k(DS_{ij})} SVL(w)}{W_k(DS_{ij})} \quad (7)$$

A severity-based weight estimation process is employed to determine severity-associated attribute weights, utilizing a three-dimensional attribute-factor (AF) tensor, WT. This tensor encapsulates the intricate relationships between attributes, users, and disease severity levels. The tensor WT undergoes decomposition as outlined in Eq. (8), where R signifies the top-rank component count, and the symbol o represents the outer product. The column vectors within factor matrices X, Y, and Z are denoted by x_r, y_r, and z_r, respectively. The dimensions of X, Y, and Z are $I \times R$, $J \times R$, and $K \times R$, correspondingly. Eq. (9) presents an element-wise equivalent of Eq. (8).

$$wt \approx \sum_{r=1}^{R} x_r^{\circ} y_r^{\circ} z_r \quad (8)$$

$$wt_{ijk} = (x_r, y_r, z_r) = \sum_{r=1}^{R} x_{ir}.y_{jr}.z_{kr} \quad (9)$$

Each row within the matrices x_r, y_r, and z_r corresponds to weight factors associated with patients, attributes, and severity levels, respectively. Disease prediction ratings, denoted as r_{ij}, are computed using the proposed prediction model, incorporating severity levels and weight vectors as defined in Eq. (10).

$$r_{ij} = \overset{T}{w}_{ij} r_{ij} = \sum_{k=1}^{K} w_{ijk}.r_{ijk} \quad (10)$$

IV. Experimental Results

The proposed disease monitoring system was engineered using Java within the NetBeans Integrated Development Environment (IDE) and leveraged the CloudSim simulation toolkit for performance evaluation. The system incorporates a standardized dataset from the University of California, Irvine (UCI) Machine Learning Repository, encompassing various diseases such as cardiovascular conditions, diabetes, and cancer. Analyzing this dataset provides a user-friendly approach to assessing disease severity, thereby contributing to the prevention of life-threatening ailments.

This section provides a detailed overview of the medical datasets employed in this study, specifically focusing on heart disease, diabetes, and cancer. Furthermore, the performance metrics utilized to evaluate the proposed health monitoring system are outlined, followed by a comprehensive presentation of experimental results. The evaluation of the suggested approach is divided into two primary domains: disease prediction and safe storage. Each domain is assessed using specific evaluation parameters.

The assessment of the secured storage component within the disease prediction system encompasses factors including decryption time, encryption time, and key generation time. The formulas for computing these times are delineated in Eq. (11), (12), and (13), respectively.

$$K = DTT + ET \quad (11)$$

$$ET = EDT - STT \quad (12)$$

$$DT = EDT - STT \quad (13)$$

In Eq. (11), DTT represents the data transferring time, while ET denotes the time required to encrypt the data. The encryption time is determined by the duration of converting the original data into its encrypted form. Fig. 2 depicts the analysis of crucial generation time for the developed secured storage system. The figure illustrates the results of five experiments conducted with varying numbers of cloud users (200, 400, 600, 800, and 1000). As observed from the graph, as the number of cloud consumers increases, the key generation time also increases.

In Eq. (12), EDT represents the end time of the encryption process, while STT signifies the start time. DT denotes the user's time spent decrypting the encrypted data, measured in milliseconds and expressed as Eq. (13).

Fig. 3 presents an analysis of the proposed algorithm's encryption time. To assess the model's performance, the evaluation involved five experiments using data sets of varying sizes: 200 KB, 400 KB, 600 KB, 800 KB, and 1 MB. As expected, the encryption time exhibited a positive correlation with data size. This is likely caused by the inherent properties

of elliptic curve cryptography used in the algorithm and the two-stage nature of the encryption and decryption processes.

Similar to the encryption process, Fig. 4 analyzes the decryption time associated with the proposed secure storage algorithm. The evaluation employed the same five data set sizes to evaluate decryption efficiency. The results demonstrate that decryption time scales proportionally with the size of the data being handled. This characteristic can be attributed to the two-stage nature of the decryption scheme employed in the method.

Fig. 5 compares the computational time required by the suggested secure storage approach and several existing systems. The evaluation employed a fixed data size of 10 GB across five scenarios. The results indicate that the proposed algorithm exhibits lower computational time than existing systems.

Fig. 6 compares the security performance of the developed secure storage algorithm (ECRS-DDA& ECC-TSEA) with several existing algorithms. The evaluation involved five experiments designed to assess the relative security of each approach. The results demonstrate that the proposed algorithm offers a superior level of protection compared to existing solutions.

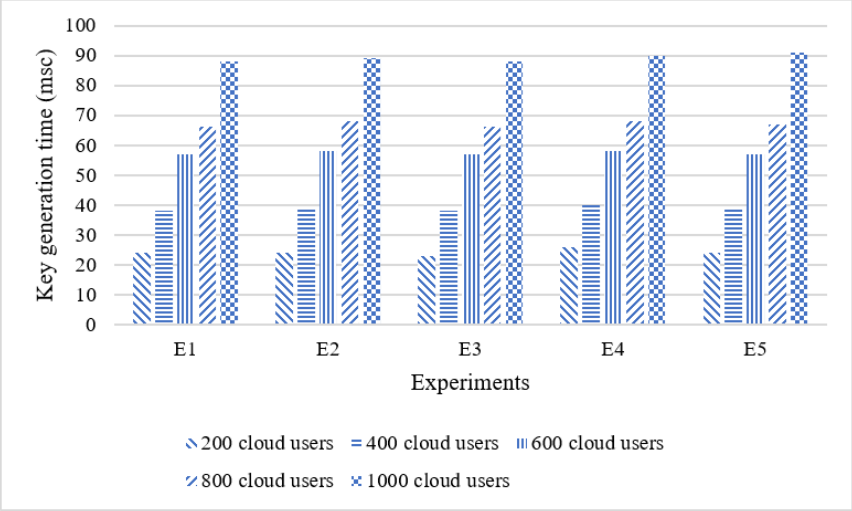

Fig. 2. Key generation time comparison.

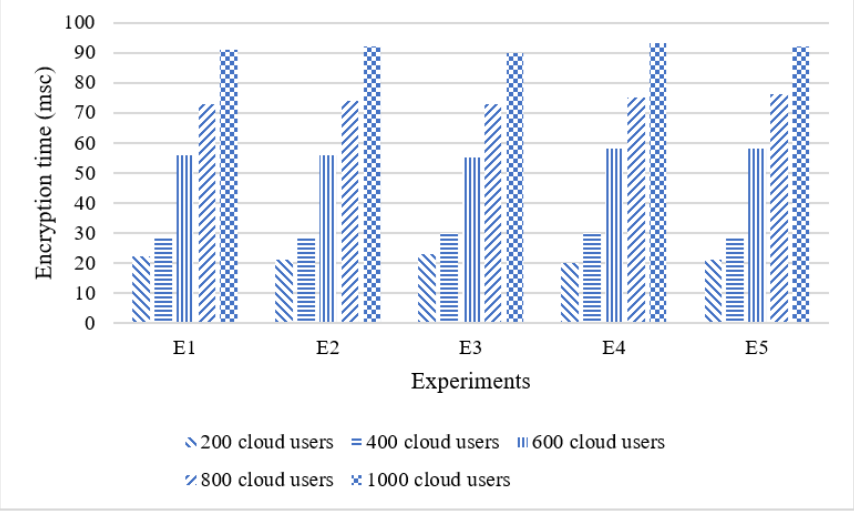

Fig. 3. Encryption time comparison.

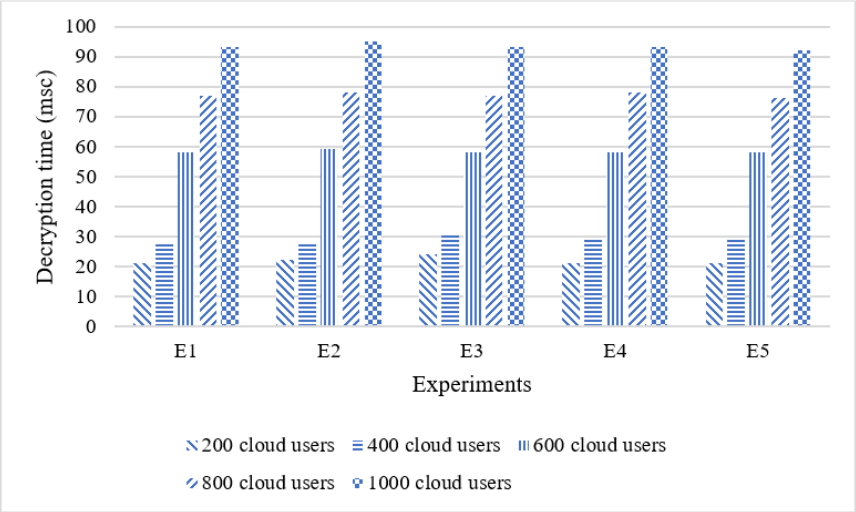

Fig. 4. Decryption time comparison.

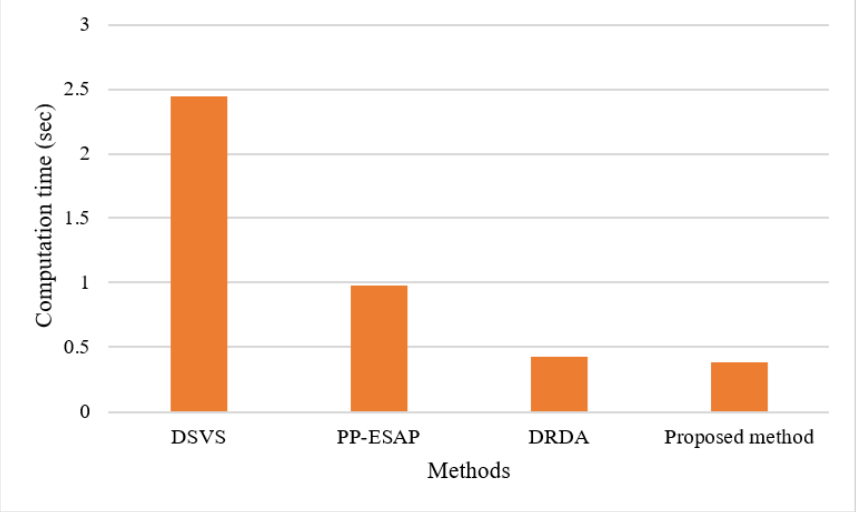

Fig. 5. Computation time comparison.

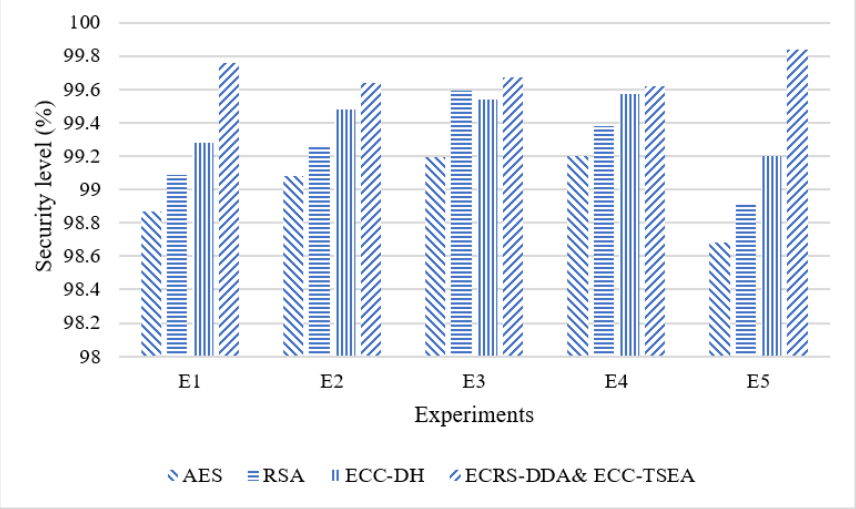

Fig. 6. Security level comparison.

V. CONCLUSION

In this research, an innovative healthcare surveillance system has been developed and deployed to assess the severity of critical illnesses, including diabetes and cardiovascular conditions. The system utilizes original data collected from patients residing in remote areas to predict disease levels. Additionally, a secure data storage model has been developed and integrated into the system to ensure the safe storage of patient data in cloud databases. Three novel algorithms have been formulated for key generation, encryption, and decryption procedures within the secure storage framework to bolster the system's security. These algorithms aim to protect sensitive patient information and prevent unauthorized access. A novel deep learning algorithm named IoT-CDLDPM has also been created and incorporated into the healthcare monitoring system. This algorithm enhances the efficiency of disease-level prediction by leveraging the power of deep learning techniques. The experimental outcomes derived from a series of trials in this study indicate the efficacy of the proposed healthcare system. The system achieved a prediction accuracy of 99.4%, demonstrating its high precision in assessing disease severity levels. Moreover, the system's security level is evaluated to be 99.7%, surpassing the performance of other healthcare systems.

REFERENCES

[1] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," Sustainability, vol. 15, no. 4, p. 3317, 2023, doi: https://doi.org/10.3390/su15043317.

[2] M. Adil et al., "Healthcare internet of things: Security threats, challenges and future research directions," IEEE Internet of Things Journal, 2024.

[3] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy-efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, vol. 34, no. 15, p. e6959, 2022.

[4] Z. Lu and X. Deng, "A cloud and IoT-enabled workload-aware Healthcare Framework using ant colony optimization algorithm," International Journal of Advanced Computer Science and Applications, vol. 14, no. 3, 2023.

[5] V. Puri, A. Kataria, and V. Sharma, "Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0," Transactions on Emerging Telecommunications Technologies, vol. 35, no. 4, p. e4245, 2024.

[6] M. Riad, "IoT-based intelligent system For Alzheimer's Disease Detection & Monitoring," International Journal of Advanced Science and Computer Applications, vol. 3, no. 2, 2024.

[7] V. Hayyolalam, B. Pourghebleh, A. A. P. Kazem, and A. Ghaffari, "Exploring the state-of-the-art service composition approaches in cloud manufacturing systems to enhance upcoming techniques," The International Journal of Advanced Manufacturing Technology, vol. 105, no. 1-4, pp. 471-498, 2019.

[8] M. Hassan, A. Hussein, A. A. Nassr, R. Karoumi, U. M. Sayed, and M. AbdelRaheem, "Optimizing Structural Health Monitoring Systems Through Integrated Fog and Cloud Computing Within IoT Framework," IEEE Access, 2024.

[9] V. Hayyolalam, B. Pourghebleh, M. R. Chehrehzad, and A. A. Pourhaji Kazem, "Single-objective service composition methods in cloud manufacturing systems: Recent techniques, classification, and future trends," Concurrency and Computation: Practice and Experience, vol. 34, no. 5, p. e6698, 2022.

[10] A. Azadi and M. Momayez, "Review on Constitutive Model for Simulation of Weak Rock Mass," Geotechnics, vol. 4, no. 3, pp. 872-892, 2024, doi: https://doi.org/10.3390/geotechnics4030045.

[11] B. Omarov, A. Tursynova, and M. Uzak, "Deep Learning Enhanced Internet of Medical Things to Analyze Brain Computed Tomography Images of Stroke Patients," International Journal of Advanced Computer Science and Applications, vol. 14, no. 8, 2023, doi: https://doi.org/10.14569/IJACSA.2023.0140874.

[12] M. D. Tezerjani, M. Khoshnazar, M. Tangestanizadeh, and Q. Yang, "A Survey on Reinforcement Learning Applications in SLAM," arXiv preprint arXiv:2408.14518, 2024, doi: https://doi.org/10.48550/arXiv.2408.14518.

[13] S. Asif et al., "Advancements and Prospects of Machine Learning in Medical Diagnostics: Unveiling the Future of Diagnostic Precision," Archives of Computational Methods in Engineering, pp. 1-31, 2024.

[14] S. Paul and C. Beulah Christalin Latha, "Machine Learning and IoT in Precision Healthcare," in IoT and ML for Information Management: A Smart Healthcare Perspective: Springer, 2024, pp. 201-234.

[15] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," Future Generation Computer Systems, vol. 110, pp. 91-106, 2020.

[16] P. D. Singh, G. Dhiman, and R. Sharma, "Internet of things for sustaining a smart and secure healthcare system," Sustainable computing: informatics and systems, vol. 33, p. 100622, 2022.

[17] N. Singh, S. Sasirekha, A. Dhakne, B. S. Thrinath, D. Ramya, and R. Thiagarajan, "IOT enabled hybrid model with learning ability for E-health care systems," Measurement: Sensors, vol. 24, p. 100567, 2022.

[18] S. A. Moqurrab et al., "A deep learning-based privacy-preserving model for smart healthcare in Internet of medical things using fog computing," Wireless Personal Communications, vol. 126, no. 3, pp. 2379-2401, 2022.

[19] A. Khanna, P. Selvaraj, D. Gupta, T. H. Sheikh, P. K. Pareek, and V. Shankar, "Internet of things and deep learning enabled healthcare disease diagnosis using biomedical electrocardiogram signals," Expert Systems, vol. 40, no. 4, p. e12864, 2023.