Hierarchical Deep Learning for Robust Cybersecurity in Multi-Cloud Healthcare Infrastructures

Tariq Emad Ali
Information and Communication Engineering, Al-Khwarizmi College of Engineering, University of Baghdad, Iraq
tariqemad@kecbu.uobaghdad.edu.iq (corresponding author)

Alwahab Dhulfiqar Zoltan
Faculty of Informatics, Eotvos Lorand University, Budapest, Hungary
dolfi@inf.elte.hu

Received: 5 September 2024 | Revised: 11 October 2024 | Accepted: 4 December 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.8918

ABSTRACT

Patient safety is in danger because healthcare networks are more susceptible to cyberattacks as they become more intricate and linked. By altering data transmitted between various system components, malicious actors can hack into these networks. As cloud, edge, and IoT technologies become more widely used in contemporary healthcare systems, this difficulty is predicted to increase. This study presents a Combined Hybrid Deep Learning Framework with Layer Reuse for Cybersecurity (CHDLCY) to address this issue. This system is built to detect malicious actions that modify the metadata or payload of data flows across IoT gateways, edge, and core clouds quickly and precisely. The CHDLCY's is a unique design demanding less training time, while bigger models at the core cloud profit from a cutting-edge layer-merging method. The core cloud model is partially pre-trained by reusing layers from trained edge cloud models, which drastically reduces the number of training epochs required from 35 to 40 to just 6 to 8. Thorough tests demonstrated that CHDLCY not only accelerates the training phase but also achieves remarkable accuracy rates, ranging from 98% to 100%, in identifying cyber threats. The proposed approach offers a significant improvement over previous models in terms of training efficiency and generalizability to new datasets.

Keywords-cloud networks; edge clouds; NFV; healthcare; DNN; autoencoders; cybersecurity

I. INTRODUCTION

The cost of medical treatment is enormous and continuously rising, with the USA spending approximately four trillion dollars in 2020, accounting for 17% of its GDP [1]. Despite these substantial investments, many countries face ineffective healthcare systems plagued by challenges such as poor chronic patient tracking, high readmission rates, delayed diagnoses, and a significant number of avoidable errors. These preventable errors remain one of the leading causes of death in the United States [2]. To address these issues and reduce rising costs, there is an increasing reliance on technology, particularly the Internet of Things (IoT), to improve healthcare outcomes through early and precise diagnoses. The projections of the International Data Corporation indicated that by 2022, 90% of medium- and large-size enterprises will have adopted cloud computing solutions, including multi-cloud and hybrid cloud environments [3]. In the healthcare sector, the use of multi-cloud technologies was expected to increase from 19% in 2019 to 37% in 2021 [4]. These advances not only improve patient survival and recovery rates by accelerating diagnosis and treatment but were also accelerated by the COVID-19 pandemic [5].

However, as analytics and data storage shift from traditional on-premises setups to edge and public clouds, the vulnerability to cyberattacks escalates [6]. Reports indicate that 91% of healthcare organizations experienced at least one cyberattack in the past two years, with breaches increasing by 71% in 2020 compared to 2019 [7-8]. The healthcare industry had the highest number of insurance claims related to ransomware attacks among major economic sectors from 2015 to 2019 [9]. Such cyber threats jeopardize patient data, placing individuals at serious risk during diagnosis, treatment, or transport. In [10], the significant impact of data breaches on 30-day hospital mortality rates was highlighted. Additionally, the targeting of critical medical equipment, such as pacemakers, poses severe threats to patient safety. For instance, the FDA recalled insulin infusion pumps due to potential manipulation [11].

As next-generation healthcare increasingly incorporates cloud computing and telecommunications virtualization, a more complex landscape emerges, presenting both opportunities and challenges. Currently, security and confidentiality concerns have limited the adoption of cloud services in healthcare to approximately 14% [12]. Traditional Intrusion Detection Systems (IDSs) are often ineffective in this context [13]. This situation underscores the pressing need for practical strategies to mitigate the increased risks of cyberattacks within next-generation healthcare systems. In response to this urgent challenge, this study proposes the CHDLCY architecture, designed to protect healthcare organizations from both internal and external threats. By leveraging a decentralized design of deep learning algorithms across edge and core clouds, CHDLCY aims to anticipate and detect data flow threats by closely monitoring transmitted data and identifying subtle changes in metadata. This innovative approach utilizes a collaborative set of neural network models across various cloud tiers, effectively addressing the expanded attack surface of modern medical facilities. Although larger and more sophisticated deep learning models improve detection accuracy, they often come with longer training times. CHDLCY tackles this issue by employing a combination of Deep Neural Network (DNN) models that significantly reduces training times for the more complex core cloud models without compromising detection accuracy. The particular contributions of this study are:

- Creates an overview framework suitable for vital medical services, such as emergency scenarios and patient care while en route.
- Creates a thorough threat model that describes dangers linked to IT and OT as well as how to mitigate them in a multi-domain next-generation healthcare architecture.
- Outlines a unique hierarchical DNN strategy to protect medical data as it moves between edge and core clouds and the IoT domain.
- Presents a merged core cloud DNN that improves predictability and training time for identifying anomalous activity in data flows.
- Carries out an exhaustive assessment of the suggested approach and offers an in-depth analysis of the results.

In addition to offering a strong defense for contemporary healthcare systems, this research shows how to use integrated and layered DNN models to achieve high detection accuracy and quick learning periods.

II. RELATED WORKS

This study presents a review of selected research, mainly from 2020 to 2024. Some earlier studies are also included for their relevance and comparative value. Some recent studies have closely examined the effectiveness of shallow Machine Learning (ML) compared to Deep Learning (DL) in security applications. As the DL detection capabilities have improved steadily, they have attracted considerable attention. Although DL often performs better than shallow ML in many areas, in [14], it was highlighted that this is not necessarily the case in cybersecurity. In [15], an intrusion detection model was presented that incorporated ML classifiers such as XGBoost, a shallow learning approach called PV-DM (Paragraph Vector-Distributed Memory), and feature selection using SHAP values (SHapley Additive explanations). This method performed exceptionally well on the UNSW-NB15 and NSL-KDD datasets. Using only four features, an excellent 98.92% accuracy was achieved on the NSL-KDD dataset, with precision, recall, and F1 scores of 98.92%, 95.44%, and 96.77%, respectively.

Many studies used DL in multicloud medical systems. For example, authors in [16] applied it in edge cloud setups with IoT sensors. Likewise, authors in [17, 18] used it with ECG classifiers to help identify and diagnose heart problems. In [19], Cognitive Fog (CF) was used to detect abnormalities medical reports. Additionally, authors in [20] explored the use of blockchain technology to help diagnose certain medical conditions BDSDT employs Ethereum smart contracts to strengthen data security and connects with the InterPlanetary File System (IPFS) for off-chain storage to control data storage costs. The verified data are then given to a DL architecture to detect intrusions in healthcare system networks. This design combined Bidirectional LSTM (BiLSTM) with the Deep-Sparse Autoencoder (DSAE). The results showed that BDSDT achieved near-perfect accuracy of 99% on two public datasets, CICIDS-2017 and ToN-IoT, outperforming existing state-of-the-art approaches in both blockchain and non-blockchain contexts.

In [21], a CNN IDS on a GPU obtained remarkable results, with 99.86% accuracy for five-class classification on the NSLKDD dataset. Similarly, in [22], a CNN model achieved 96.55% accuracy on the CICIDS2017 dataset. However, this method used only one flat cloud structure and emphasized the importance of model training durations. In [23], a DL traffic cyberattack prediction and data offloading method (DLTPDO-CD) was introduced. A DBN adjusted with the Barnacles Mating Optimizer (BMO) approach achieved 97.65% accuracy. In [24], accuracy rates of 96.7% and 98.5% were achieved using CNN and LSTM networks. In [25], an Autoencoder (AE)-based retrieval module was used in conjunction with a CNN-based supervised pretraining module to achieve accuracies of 89.45% and 80.25% for benign and defect flow in different datasets. Using the Plant Pathology 2020 dataset, AEs were used in [26] to achieve 95% training and more than 90% validation accuracy in agricultural settings. In [27], a thorough examination of DL and ML methods was carried out to precisely identify and categorize microorganism images on a larger scale. The CNN method performed better than other approaches on a dataset consisting of eight different species of microorganisms.

These results demonstrate that although DL has seen occasional success in network intrusion detection, the area is still in its early stages of development. Utilizing a combined approach to stacked distributed systems in multiple cloud situations has attracted little focus. Although some first ideas of hierarchical neural networks in essential services were presented in [28], this study provides a more thorough and validated implementation in this domain.

III. PROPOSED HEALTHCARE FRAMEWORK

The design of a medical facility framework provides significant information for improving the systems and aids in understanding the data flow. With this configuration, a threat model and targeted protections for the cyber-physical system under investigation may be constructed. The infrastructure is segmented into three primary domains: IoT, multi-cloud, and visualization, as illustrated in Figure 1.

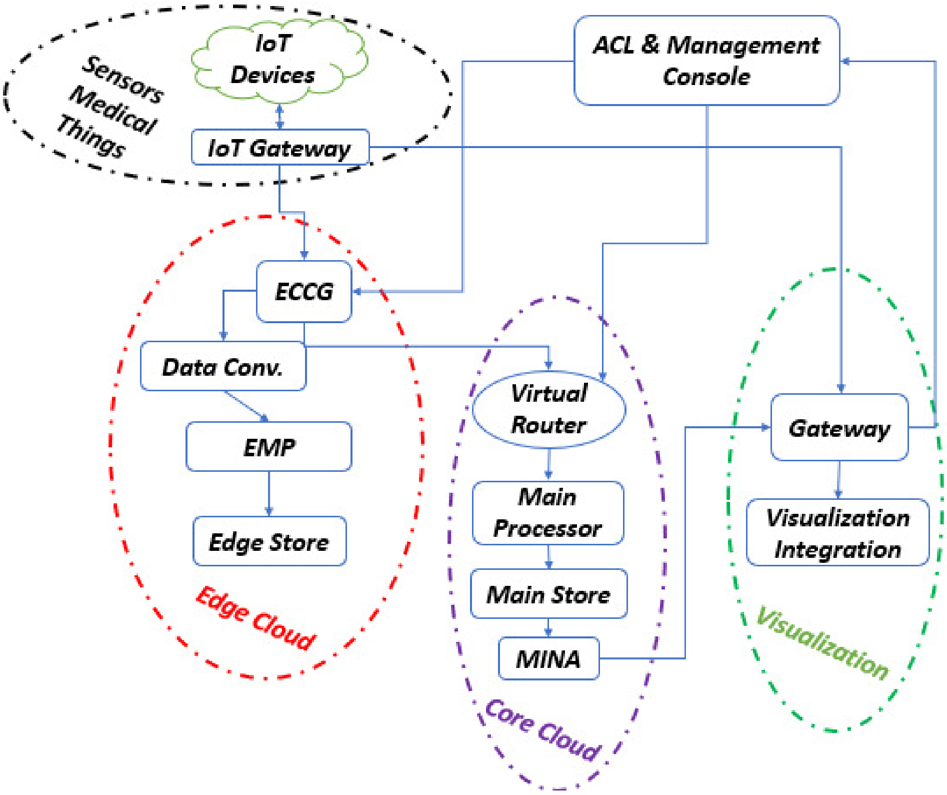

Fig. 1. Architecture of the proposed next-generation healthcare system.

Virtual Network Services (VNS), or contemporary wide area network services, can be used for data transfer between various domains. ISPs are expected to use VNS more extensively. The IoT sector includes a wide range of wired and wireless devices, such as actuators, wearables, swallowed devices, etc., intended to collect and distribute patient data. These sensors monitor vital indicators such as blood pressure, heart rate, and oxygen saturation. IoT devices can automatically convey alerts and suggestions to paramedics for patients in ambulances [29]. This area typically performs the roles of an input, producing large amounts of multidimensional patient data, and a sink for instructions that are sent to actuators and other devices.

However, the short battery life, low computing power, and small memory of IoT devices provide operational challenges, making them dependent on the multi-cloud domain to provide extra processing, analytics, and storage capacity. Situated at the boundary of this domain, the IoT gateway serves as a GUI between the cloud and the IoT domain, facilitating operations such as data translation and protocol management as required. The computing or cloud domain in the proposed framework is organized into a hierarchy of edge and core clouds. The closest cloud to the patient is an edge cloud, run by mobile service providers using servers mounted on mobile towers adjacent to base stations. These close clouds manage workloads that profit from proximity to IoT devices and offer low-cost and high-latency connections to the multi-cloud system. Core clouds, also known as public clouds, provide large amounts of historical data storage along with sophisticated analytics features. For long-term storage, edge-cloud data collected for active monitoring or diagnostics can be moved to core clouds. Core clouds have higher latency and connectivity costs than edge clouds, but can analyze massive amounts of historical and real-time patient data utilizing advanced AI-based analytics. Finally, data ingestion in many representations is the core function of the visualization domain. Clinical personnel use these data to monitor patient health, find abnormalities and exceptions, and recognize early warning indicators [30]. Although the primary focus of this area is processed data, commands, instructions, and prescriptions can also create tiny amounts of data. This approach can help in fast and precise diagnoses by providing clinical professionals with different data streams in tabular, graphical, and other forms. Using ambulance data, physicians can instantly consult with medics to provide patient care recommendations. Improved visualizations aid in more accurate diagnoses and successful therapy outcomes.

The framework in Figure 1 aims to provide medical programs that manage patient care devices with complete data. It includes all the necessary features, including telemedicine, analytics, communication, remote consultations, and image collection. As a result, large amounts of data are sent for processing and preservation to the IoT-Cloud space. The proposed design is scalable and versatile, able to keep up with growing system requirements while maintaining strong security. It is organized into four linked domains. This segmentation facilitates the development of modular security rules throughout the healthcare network. The following are important elements in each of these domains.

A. IoT Gateway

Existing in homes, offices, hospitals, and ambulances, IoT gateways act as a link between the edge cloud and IoT domains. These routers maintain cloud connectivity and manage important functions, including data transformation and protocol handling. They may interact with edge clouds or core clouds straight away, and they can link to the virtual or physical wide area network of the service provider.

B. Gateways to the Edge-Core Clouds (GECC)

These gateways offer workload allocation, numerous capacity possibilities, and data compression for faster transmission. They collect telemetry data by connecting IoT gateways and devices. Physical or virtual routers (vRouters) can serve as gateways.

C. Edge and Main Processors (EMP)

With enough processing capacity and often particular hardware, such as edge tensor processing units, edge processors oversee data streams from devices or gateways. They can train and use smaller neural network models. Patient data are temporarily stored in edge storage during ambulance transit or when there is a need for quick data access. Core cloud computers, in the meantime, manage sophisticated analytics by analyzing both recent and historical data using sizable neural network models. They provide a thorough data display and analysis by integrating various information sources with the visualization area.

D. Agents for Artificial Intelligence (AAI)

Along with the main processor, the core cloud domain typically consists of sophisticated software for historical data analysis and specialized hardware such as GPUs. This configuration helps in the detection of new diseases and the prediction of patient readmissions.

E. Visualization

This area offers solutions for handling, tracking, and diagnosing patients by displaying their data. Many information sources are combined and synthesized, providing healthcare professionals with crucial insights. It facilitates the process of making better decisions by drawing attention to patterns and relations that are not immediately obvious from raw data or reports.

F. Access Control (ACL)

Authorization, authentication, and accounting for connections made by both persons and devices are managed by access control, which prevents data from being accessed without authorization, whether it comes from core or edge clouds.

G. Provisioning, UI, and Other Tools (i.e., Management Console)

These solutions give area controllers a straightforward interface for allocating cloud resources and injection policies. This approach enhances end-to-end security by providing consistent protection across all domains and reducing the need for manual provisioning. It also ensures patient safety, regulatory compliance, high availability, and improved patient care, whether in transit or at home. The main goal of this study is to develop an anomaly detection system that uses stacked DL to identify vulnerabilities in data flow between the edge and core clouds or the IoT_EdgeCloud. Strong and reliable authentication is critical to secure patient data and related information. A promising solution for patients in emergencies, such as in ambulances, is the use of brain wave biometrics.

Integrating biometric methods with cryptographic techniques to implement AAA ensures strong protection. This study uses public-key cryptography combined with advanced hashing algorithms, including Stacked Sparse Autoencoder (SSAE) [31], to achieve this goal.

$L(z^1, z^2) = \frac{1}{2} \parallel z^1 - z^2 \parallel^2$ is the loss function that is trained to minimize the MSE between z^1 and z^2. This is the input and the output for the second hidden layer.

$z^2 = f\left(w^1 z^{(1)^T}\right)$ is the output vector. This procedure is repeated up to the last hidden layer that is linked to the output layer. For n hidden layers, the output vector is:

$$y' = f\left(\omega^n z^{(n)^T} + b^n\right) \qquad (1)$$

SSAE can be improved using training samples in the format (x, y) (or feature vectors, output vector), where y is the ground truth from training samples (x, y). The weights linking the n^{th} trained layer to the output layer are used, predictions y' are derived, and all weights are altered to minimize $\frac{1}{2}\|y - y'\|^2$. During the last process, all weights are refined. A regularization term is introduced to reduce the MSE in the overall cost function:

$$J(w, b) = \frac{1}{n}\sum_i (MSE) + \lambda\Omega_w + \beta\Omega_{sparsity} \qquad (2)$$

The third element is the small amount of regularized information (with coefficient β) that restricts the outcome of the hidden layer to be sparse. The initial element is the MSE averaged over all training samples. The second term applies a regularization to the weights to keep the regularizer from becoming too small. Kullback-Leibler Divergence (DKL) is a commonly used regularization that provides considerable value when the neuron's activity is not at the expected level. Each SSAE's associated weights and biases are variables that can be learned. To achieve acceptable results, hyperparameters, such as the number of layers, neurons, and loss function parameters, must be properly adjusted. Table I lists several of the hyperparameters and their common values used.

TABLE I. SSAE HYPERPARAMETERS

Measurement	Synopsis	Normal value(s)
No. of layers	Determines the neural network's depth	4, 12
Quantity of neurons in every single layer	Reduce from the input layer to the output layer, then symmetrical raise	60, 180
Code size	Outermost level with a highly condensed source description	30
Loss function	MSE	
λ	Regularization factor	0.00000001
B	Sparsity regularizer	0.2
β_1, β_2	Adam optimization decay rates	0.8, 0.9

Unlabeled data are used to train one layer of DNN at a time. A network can avoid simple symmetric local optima by starting it with modest random weights (e.g., evenly between -0.1 and 0.1). The reconstruction error serves as a signal of normality or abnormality in the data flow, as the SSAE is trained solely on normal events. After training, the SSAE fails to rebuild anomalous data and instead reconstructs regular data flows with a low Root Mean Square Error (RMSE). The dataset is divided into one or more test datasets and a training dataset. Training ends when the RMSE regularly falls below a predetermined threshold. The trained model is then tested using the test dataset. To avoid overfitting, the network is frequently cross-validated throughout training. The number of epochs needed to obtain an error minimum is commonly used to indicate the duration of the training. The evaluation portion covers hyperparameter settings.

IV. PROPOSED FRAMEWORK IMPLEMENTATION AND VALIDATION

SSAEs were employed to train an intrusion detection classifier, comparing its performance with classical classifiers such as SVM, Naive Bayes (NB), DT, and Random Forest (RF), and evaluating the training time and detection accuracy of CHDLCY with standard DNNs. Finally, a hierarchical multi-cloud framework is presented for securing data in motion, with attention on the boundaries of edge and core clouds.

The CHDLCY model was tested on various datasets, including the NSL-KDD dataset [32], containing 41 features. To evaluate the model's performance, metrics such as accuracy, precision, recall, F1-score, training time, false positives, and false negatives were analyzed.

Different scenarios were tested to achieve the best results. The code was implemented using an edge-cloud model with Keras and TensorFlow.

In summary, CHDLCY provides a distributed, hierarchical deep-learning framework to secure data in transit within a multi-cloud environment. Leveraging SSAEs, it ensures fast and accurate intrusion detection across all cloud levels. Its hierarchical structure offers a scalable and efficient solution for real-time applications, improving detection accuracy while minimizing training time.

V. EVALUATION AND RESULTS

This paper used two datasets (DSs), namely a Public DS and a Synthetic DS to estimate the efficiency of the proposed model.

A. Public Dataset

The BOT-IoT-DS, unconstrained in Nov. 2018 by the UNSW Canberra Cyber Centre, is considered to imitate genuine IoT network traffic and occurrence scenarios. This DS using practical network formations and outdone IoT devices, bests older DS like KDDCup99 and NSL-KDD by containing a extensive series of recent outbreak methods. The dataset contains nine outbreak attack types such as DoS, Reconnaissance, and Fuzzer in conjunction with standard circulation, letting indistinct discrepancy amongst malicious and legitimate activities. With 48 traffic-related features, it assists as a strong reserve for rising and difficult IDS tailored for IoT spheres. Recognized for its accurate simulation of IoT devices and outbreaks, the BOT-IoT DS is widely used for evolving difference exposure and pretty IoT cybersecurity.

B. Data Produced on the Testbed

Figure 2 illustrates the production of a healthcare-specific dataset using botnet attacks, although the BOT-IoT dataset is composed of semantic info from a variety of IoT devices. The testbed setup includes:

- IoT Domain: An external Ethernet shield and an Arduino Mega microcontroller are used for medical IoT sensors.
- Network Domain: Three machines and the microcontroller are connected via an Ethernet switch on an internal network.
- Visualization Domain: An Ubuntu Linux server to view metadata and information regarding patients.
- Attacker Domain: A Kali Linux-powered server for emulating harmful operations, such as dataflow manipulation and sniffing.

C. Infrastructure for Deployment and Development Tools

Numerous hardware and software platforms were used to evaluate the edge and core models. Some of the code was converted to MATLAB from Python on the Jupyter Notebook platform. The method was evaluated on a Windows 10 PC and a Mac 8-core CPU. The models were also trained and tested on Google Colab with TensorFlow V2.x and Keras during the review process, using CPUs and GPUs such as Nvidia L70s, T5s, P5s, and P300s. The aforementioned testbed was utilized to create botnet attack and normal data, anonymize it, and record it across some sessions. A Kali Linux system was used to mimic attack data, and the Argus Network Management System [35] was used to extract metadata. Weka [36] was used to rate the data.

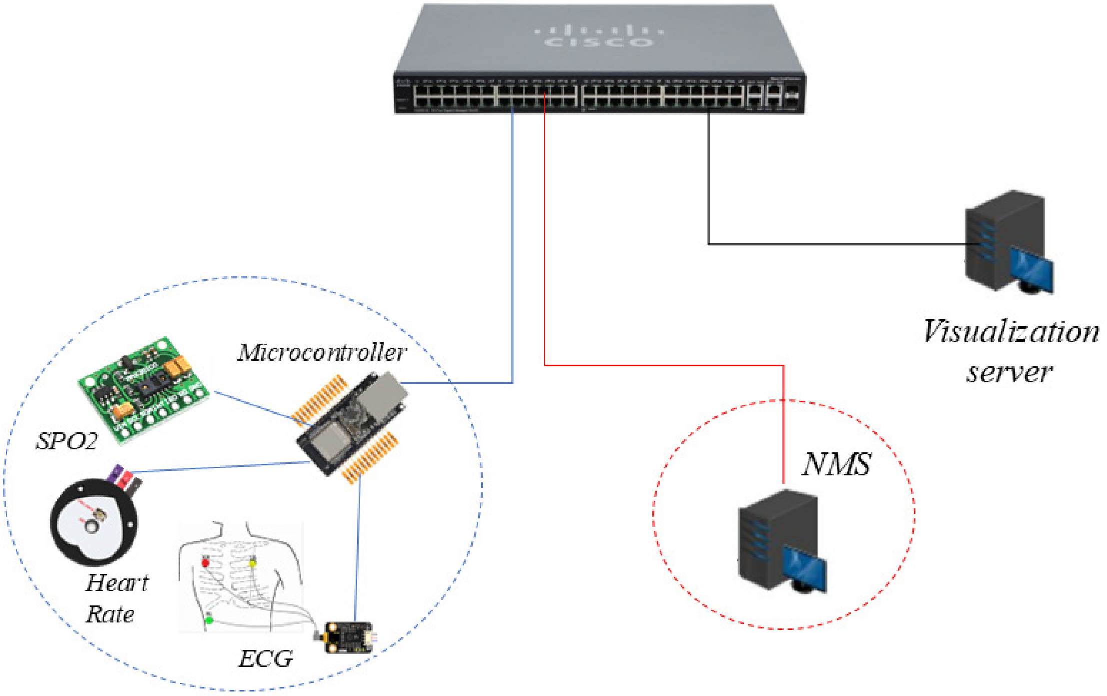

Fig. 2. Healthcare testbed for dataset generation.

D. Results

1) Training and Assessment at the Edge Clouds

In this setup of the stacked AE for training in edge clouds, the dataset was randomized by shuffling its records before feeding it into the model. To achieve this, built-in functions from ML libraries, such as Python's NumPy shuffle function, were used. This ensures that the data do not follow any particular order, preventing potential biases during training.

Randomization helps the model to generalize better by avoiding overfitting to any specific sequence in the data. This approach enables the model to learn diverse and robust features, essential for high performance in real-world edge cloud environments. As shown in Figure 3, the model, when tested on unseen datasets, demonstrated excellent generalization, with training and test losses converging within 20-60 epochs.

2) Training and Assessment at the Core Cloud

Figure 4 displays the results for the integrated model in the core cloud. When compared to edge cloud learning, cross-trained models stabilize more quickly (in less than four instead of five epochs). The layer reuse from the edge clouds contributes significantly to the efficiency and reliability benefits.

3) Training Time Analysis

For neural network models, the computational demand study revealed a high order of complexity O(n^5). The edge cloud models take roughly 125 seconds for 4,000 training and 1,000 testing on an Nvidia Quadro 8GB M4000 GPU, which is faster than the baseline findings in [27]. The training time is notably reduced by the combined model with twelve layers, which reuses edge-trained layers, compared to the uncombined core model with eight layers and a deeper depth (see Table II).

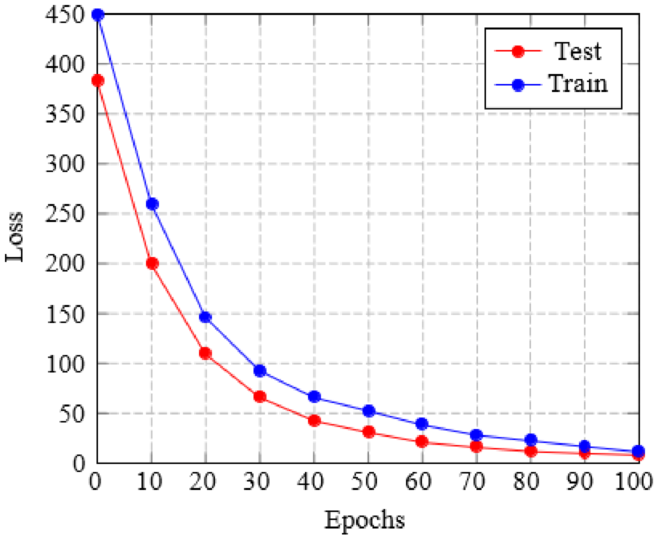

Fig. 3. Loss vs. Epochs for the cloud edge model.

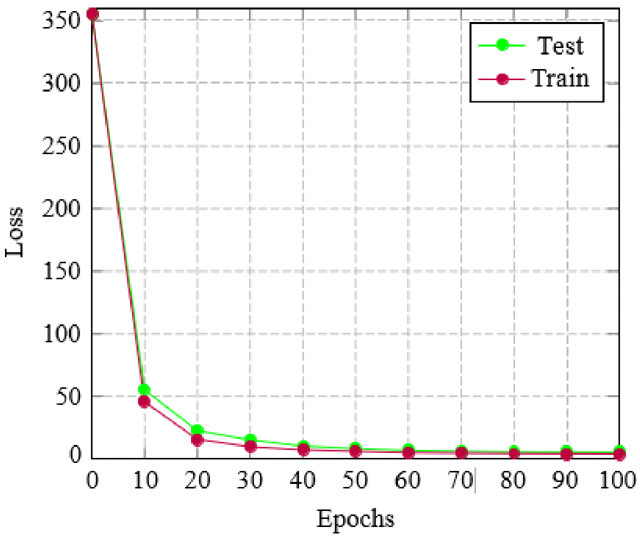

Fig. 4. Loss vs. Epochs for the cloud core model.

TABLE II. TRAINING TIME COMPARISON

Model	Epochs	Training time (s)
Unmerged 8-layer	100	5000
Merged 12-layer	100	3200

4) *Training and Testing Accuracy*

Table III presents the training and evaluation accuracy for the edge and core cloud environments. The edge cloud exhibits a testing accuracy of 95.23% and a training accuracy of 96.36%. On the other hand, the core cloud demonstrates a testing accuracy of 99.75% and a training accuracy of 99.80%. These results indicate that while the core cloud configuration achieves higher accuracy in both training and testing phases, the edge cloud may offer better overall effectiveness in practical scenarios due to its closer proximity to data sources, resulting in lower latency that can enhance learning.

TABLE III. TRAINING AND TESTING ACCURACIES FOR CLOUD AND EDGE MODELS ON THE DATASETS

Cloud Model	Accuracy (%)	
	Testing	Training
Edge	95.23	96.36
Core	99.75	99.80

5) *CHDLCY Method's Effectiveness in Detecting Attacks*

The testbed and UNSW datasets were used to evaluate the model's performance in intrusion detection. Table IV summarizes the results, which were obtained using attack situations that impact metadata. The system achieved high accuracy (98-100%), a low false positive rate (0.5%), and a notable improvement over the unmerged model (95-97%).

TABLE IV. CONFUSION MATRIX FOR ATTACK DETECTION

No.	Attack	Normal	Attack	Normal	Total	Accuracy
	(TP)	(FN)	(FP)	(TN)	Vectors	(%)
1	200	0	19	355	574	96.69
2	188	0	0	511	699	100.00
4	96	0	3	232	331	99.09
5	92	16	0	184	292	94.52
6	100	0	0	280	380	100.00
7	80	17	0	243	340	95.00
8	110	1	1	287	399	99.50
9	27	1	1	100	129	98.45
10	126	12	0	398	537	97.76

VI. CONCLUSION

This study emphasizes how DL, more specifically ANNs, can be used to identify attacks in a variety of settings. Although these models have been the subject of many studies, relatively few of them discuss their use in cloud or multi-cloud contexts. To the greatest extent of our understanding, not much research has been done on IoT-multi-cloud infrastructures, particularly when it comes to merged and hierarchical AEs with layer reuse. The proposed CHDLCY system successfully closes this gap. The hierarchical structure of this model is in line with the organization of healthcare networks. Models that scale in complexity were used from IoT devices to core clouds, optimizing the implementation based on the processing power at each stage, using a distributed IDS.

The temporal complexity of sophisticated deep learning models is a prevalent problem. This proposal involves utilizing learned layers from edge clouds on the core clouds, which is a unique way to address this problem. This approach allows large neural network models to train faster, reducing the number of factors that must be learned in core clouds. The proposed strategy significantly improved the efficacy of training. Compared to an eight-layer uncombined model without edge cloud training, a twelve-layer combined model that reuses trained layers from edge cloud models reduces training time by 10.1% to 29.2%. Moreover, the accuracy of the merged models, routinely exceeded 98%, frequently reaching 98-100%, whereas the accuracy of the unmerged models was 95-97%. Combined models trained on a mix of recent data from IoT gateways and edge clouds and previous patient data from core clouds are expected would perform comparably in real-world applications.

The CHDLCY system is designed to be scalable and adaptable, capable of detecting medicine problems techniques not included in the UNSW-NB15 dataset. In healthcare, where patient lives and well-being are at stake, deep learning systems must provide clear and justifiable conclusions. Healthcare providers need to critically evaluate and understand the reasoning behind any diagnosis or prognosis these systems offer. This transparency can build trust and encourage adoption of such technologies. Future research should aim to enhance and expand this approach to address these challenges and further strengthen its capabilities.

ACKNOWLEDGMENT

This study was supported by the EKÖP-24 University Excellence Scholarship Program of the Hungarian Ministry for Culture and Innovation from the source of the National Research, Development, and Innovation Fund.

REFERENCES

[1] "National health expenditure data: NHE fact sheet," Center for Medicare and Medicaid Services. http://www.cms.hhs.gov/NationalHealthExpendData/25_NHE_Fact_Sheet.asp.

[2] F. I. Ali, T. E. Ali, and A. H. Hamad, "Telemedicine Framework in COVID-19 Pandemic," in *2022 International Conference on Engineering and Emerging Technologies (ICEET)*, Kuala Lumpur, Malaysia, Oct. 2022, pp. 1–8, https://doi.org/10.1109/ICEET56468.2022.10007389.

[3] R. Zorgati, H. Hassen, and K. A. Alsulbi, "The Deployment of E-Learning Application as a Web Service in a Cloud Broker Architecture," in *Advanced Information Networking and Applications*, Cham, 2024, pp. 1–12, https://doi.org/10.1007/978-3-031-57916-5_1.

[4] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, and R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," *Applied Soft Computing*, vol. 118, Mar. 2022, Art. no. 108439, https://doi.org/10.1016/j.asoc.2022.108439.

[5] F. I. Ali, T. E. Ali, and Z. T. Al_dahan, "Private Backend Server Software-Based Telehealthcare Tracking and Monitoring System," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 01, pp. 119–134, Jan. 2023, https://doi.org/10.3991/ijoe.v19i01.32433.

[6] G. Alotibi, "A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13787–13795, Apr. 2024, https://doi.org/10.48084/etasr.7123.

[7] C. Kowalkowski, J. Wirtz, and M. Ehret, "Digital service innovation in B2B markets," *Journal of Service Management*, vol. 35, no. 2, pp. 280–305, Dec. 2023, https://doi.org/10.1108/JOSM-12-2022-0403.

[8] "2024 Data Breach Investigations Report," *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir/.

[9] “Cyber Claims Study 2020 Report,” *NetDiligence*, Nov. 11, 2020. https://netdiligence.com/cyber-claims-study-2020-report/.

[10] S. J. Choi and M. E. Johnson, "Do Hospital Data Breaches Reduce Patient Care Quality?" arXiv, Apr. 03, 2019, https://doi.org/10.48550/arXiv.1904.02058.

[11] T. E. Ali, Y.-W. Chong, and S. Manickam, "Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN," *Applied Sciences*, vol. 13, no. 5, Jan. 2023, Art. no. 3033, https://doi.org/10.3390/app13053033.

[12] T. E. Ali, Y. W. Chong, and S. Manickam, "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review," *Applied Sciences*, vol. 13, no. 5, Jan. 2023, Art. no. 3183, https://doi.org/10.3390/app13053183.

[13] T. Emad Ali, F. Imad Ali, A. Hussein Morad, and M. A Abdala, "Diabetic Patient Real-Time Monitoring System Using Machine Learning," *International Journal of Computing and Digital Systems*, vol. 16, no. 1, pp. 189–199, 2024.

[14] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021, https://doi.org/10.1109/ACCESS.2021.3054129.

[15] C. E. L. Asry, I. Benchaji, S. Douzi, and B. E. L. Ouahidi, "A robust intrusion detection system based on a shallow learning model and feature extraction techniques," *PLOS ONE*, vol. 19, no. 1, 2024, Art. no. e0295801, https://doi.org/10.1371/journal.pone.0295801.

[16] V. Hayyolalam, M. Aloqaily, Ö. Özkasap, and M. Guizani, "Edge Intelligence for Empowering IoT-Based Healthcare Systems," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 6–14, Jun. 2021, https://doi.org/10.1109/MWC.001.2000345.

[17] H. Elayan, M. Aloqaily, and M. Guizani, "Digital Twin for Intelligent Context-Aware IoT Healthcare Systems," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16749–16757, Sep. 2021, https://doi.org/10.1109/JIOT.2021.3051158.

[18] F. Zaman, M. Aloqaily, F. Sallabi, K. Shuaib, and J. B. Othman, "Application of Graph Theory in IoT for Optimization of Connected Healthcare System," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Taipei, Taiwan, Dec. 2020, pp. 1–6, https://doi.org/10.1109/GLOBECOM42002.2020.9322157.

[19] M. Al-Khafajiy *et al.*, "Intelligent Control and Security of Fog Resources in Healthcare Systems via a Cognitive Fog Model," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–23, Aug. 2021, https://doi.org/10.1145/3382770.

[20] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83, Feb. 2023, https://doi.org/10.1016/j.jpdc.2022.10.002.

[21] S. Hizal, U. Cavusoglu, and D. Akgun, "A new Deep Learning Based Intrusion Detection System for Cloud Security," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, Jun. 2021, pp. 1–4, https://doi.org/10.1109/HORA52670.2021.9461285.

[22] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, "A Novel Network Intrusion Detection System Based on CNN," in *2020 Eighth International Conference on Advanced Cloud and Big Data (CBD)*, Taiyuan, China, Dec. 2020, pp. 243–247, https://doi.org/10.1109/CBD51900.2020.00051.

[23] T. E. Ali, F. I. Ali, N. Pataki, and A. D. Zoltán, "Exploring Attribute-Based Facial Synthesis with Generative Adversarial Networks for Enhanced Patient Simulator Systems," in *2024 7th International Conference on Software and System Engineering (ICoSSE)*, Paris, France, Apr. 2024, pp. 53–60, https://doi.org/10.1109/ICoSSE62619.2024.00017.

[24] Y. Xun, J. Qin, and J. Liu, "Deep Learning Enhanced Driving Behavior Evaluation Based on Vehicle-Edge-Cloud Architecture," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6172–6177, Jun. 2021, https://doi.org/10.1109/TVT.2021.3078482.

[25] M. He, X. Wang, J. Zhou, Y. Xi, L. Jin, and X. Wang, "Deep-Feature-Based Autoencoder Network for Few-Shot Malicious Traffic Detection," *Security and Communication Networks*, vol. 2021, no. 1, 2021, Art. no. 6659022, https://doi.org/10.1155/2021/6659022.

[26] H. Elayan, M. Aloqaily, and M. Guizani, "Digital Twin for Intelligent Context-Aware IoT Healthcare Systems," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16749–16757, Sep. 2021, https://doi.org/10.1109/JIOT.2021.3051158.

[27] S. Khasim, H. Ghosh, I. S. Rahat, K. Shaik, and M. Yesubabu, "Deciphering Microorganisms through Intelligent Image Recognition: Machine Learning and Deep Learning Approaches, Challenges, and Advancements," *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024, https://doi.org/10.4108/eetiot.4484.

[28] L. Gupta, "Hierarchical Deep Learning for Cybersecurity of Critical Service Systems," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom, Jul. 2020, pp. 346–351, https://doi.org/10.1109/WorldS450073.2020.9210361.

[29] A. Dhulfiqar, N. Pataki, and M. Tejfel, "Chatbot-Based Querying of IoT Devices in EdgeX," presented at the SQAMIA 2023: Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications, Bratislava, Slovakia, Sep. 2013.

[30] F. Eyvazov, T. E. Ali, F. I. Ali, and A. D. Zoltan, "Beyond Containers: Orchestrating Microservices with Minikube, Kubernetes, Docker, and Compose for Seamless Deployment and Scalability," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, Mar. 2024, pp. 1–6, https://doi.org/10.1109/ICRITO61523.2024.10522382.

[31] Y. Imrana, Y. Xiang, L. Ali, A. Noor, K. Sarpong, and M. A. Abdullah, "CNN-GRU-FF: a double-layer feature fusion-based network intrusion

detection system using convolutional neural network and gated recurrent units," *Complex & Intelligent Systems*, vol. 10, no. 3, pp. 3353–3370, Jun. 2024, https://doi.org/10.1007/s40747-023-01313-y.

[32] S. Attar-Khorasani and R. Chalmeta, "Internet of Things Data Visualization for Business Intelligence," *Big Data*, vol. 12, no. 6, pp. 478–503, Dec. 2024, https://doi.org/10.1089/big.2021.0200.

[33] J. M. E. Gray, "Codified Disparity: The Medicaid IMD Exclusion, Mental Health Parity, and Congressional Intent," *Indiana Health Law Review*, vol. 21, 2024, Art. no. 227.

[34] K. Hacker, "The Burden of Chronic Disease," *Mayo Clinic Proceedings: Innovations, Quality & Outcomes*, vol. 8, no. 1, pp. 112–119, Feb. 2024, https://doi.org/10.1016/j.mayocpiqo.2023.08.005.

[35] C. Min, J. Yi, U. G. Acer, and F. Kawsar, "Enabling Cross-Camera Collaboration for Video Analytics on Distributed Smart Cameras." arXiv, Jan. 27, 2024, https://doi.org/10.48550/arXiv.2401.14132.

[36] X. Zhou, "Data Mining of the Underachievers' Performance of E-learning and Finals in College English with SPSS and WEKA," in *2024 5th International Conference on Computer Engineering and Application (ICCEA)*, Hangzhou, China, Apr. 2024, pp. 767–770, https://doi.org/10.1109/ICCEA62105.2024.10603788.