Journal of Computational and Experimental Science (JCES)
ISSN Print: XXXX | ISSN Online: XXXX
Volume 1, Number 1, 2026, Pages 89-103
Journal Home Page: https://journals.airsd.org/index.php/jces

OPTIMIZATION PERFORMANCE OF CYBERSECURITY WITHIN MULTI-MODAL CLOUD HEALTHCARE INDUSTRY BASED ON DEEP LEARNING TECHNIQUES

Muhammad Irfan Balouch[1], Syed Sohail Ahmed Shah[1*], Salman Qazi[1], Sana Nisar Shaikh[1]
[1] *Department of Computer Science, Faculty of Computing & Information Technology, Government College University Hyderabad*

ARTICLE INFO

Article History:
Received: April 28, 2026
Revised: May 10, 2026
Accepted: May 25, 2026
Available Online: June 18, 2026

Keywords:
Cybersecurity, Healthcare, Internet of Things (IoT), multi-modal, and cloud architectures

Corresponding Author:
Syed Sohail Ahmed Shah
Email:
sohailahmed.shah@gcuh.edu.pk

ABSTRACT

In next-generation medical systems, the amount of Internet of Things (IoT) devices, edge computing infrastructure, and multi-modal cloud architectures has increased significantly, making healthcare cybersecurity a global concern. Although healthcare organizations invest a lot in storing security measures, they are far more susceptible to the sophisticated cyber threats. More than 90% of them have experienced at least one cyberattack over the past few years, and between 2013 and 2023, ransomware attacks in the healthcare industry have seen a surge to unprecedented heights. There is an important gap in the current literature: current cybersecurity frameworks don't offer a unified, scalable, and efficient solution for securing real-time flows of data across the different layers of the IoT, across the shore (edge) clouds, and across the center (core) clouds in a multi-domain healthcare environment. The current models are either computation intensive or domain specific, with multi-modal healthcare architecture being under-protected. This study introduces a novel hierarchical Deep Neural Network (DNN) framework that can identify and block malicious activities in multi-area healthcare data flows. The framework is inspired by transfer learning, utilizing pre-trained edge cloud models and fusion is to an optimized center cloud model. A Capability List (CP List) access control mechanism is built-in to implement fine-grained data access policies. The proposed model is tested on the structured dataset of healthcare network security incidents from the simulated environments in 2024. The experimental results show that the proposed hierarchical DNN architecture can achieve the accuracy of 95% to 100% for training and testing in the unknown attack. Taking an average of 26.2% less training time than the independently trained center cloud models, the model needs just 6-8 epochs to train, whereas the standalone edge cloud model requires 35-40 epochs. The research has validated that the combination of hierarchical deep learning and cloud-based security systems can greatly improve threat detection and decrease computational load. To protect sensitive patient data, the use of hierarchical AI-driven security is recommended, as well as the standardization of multi-layer access control across all IoT, edge and cloud environments for policymakers and healthcare administrators.

1. INTRODUCTION

In the context of Information Technology (IT) and cloud computing, cybersecurity is one of the most critical issues facing organizations in a digitally integrated environment, especially in the healthcare industry. Cybersecurity is the application of technologies, processes, and organizational practices to protect computer systems, networks, programs, and data from unauthorized access, damage, theft, or disruption. Within the healthcare sector, it involves safeguarding Electronic Health Records (EHRs), communications between medical devices, clinical decision-making applications, and the substantial amounts of patient-sensitive information flowing across multi-cloud environments with IoT integration.

Cloud computing, with its five key building blocks: on-demand computing, elasticity, rapid adaptation, geographic independence, and cybersecurity, has ushered in a paradigm shift in the collection, storage, processing, and sharing of healthcare data. Cloud-based solutions are increasingly becoming a staple in the healthcare industry, with their three main service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each presenting unique security challenges in shared resource environments, data sovereignty, and access control. The increased reliance on IoT medical devices, wearables, remote-monitoring sensors, and edge computing nodes compounds the security challenge by extending the attack surface beyond network perimeters to distributed, typically resource-constrained endpoints.

The larger picture of healthcare cybersecurity is characterized by a rapidly changing threat landscape, in which cyberattacks are becoming increasingly sophisticated and prevalent. In 2020, the United States spent $4.1 trillion on health care, accounting for 19.7% of its GDP, yet many medical errors are preventable and can be exacerbated by cyber incidents, which are a primary driver of patient harm. More than 90% of healthcare organizations have been victims of a cyberattack at least once, with a 71% increase in attacks from 2020 to 2023. Healthcare had the highest number of ransomware insurance claims among all economic sectors from 2013 to 2023, underscoring its importance as a high-value target for attackers. Healthcare systems are becoming multi-domain, multi-layer environments where the traditional perimeter security approach is simply not enough due to the convergence of cloud, IoT, and big data. They have edge computing nodes, known as shore clouds, which process data close to the source to minimize latency and facilitate real-time clinical response, and central clouds for storing large-scale data, data analysis, and administrative work. The interdependence of these layers introduces intricate dataflow paths that are highly vulnerable to man-in-the-middle attacks, payload tampering, unauthorized data exfiltration, and service disruption.

Despite the extensive research in the areas of cloud security, IoT protection, and intrusion detection, a fundamental research challenge remains: the lack of a single cybersecurity framework using Deep Learning that supports the security needs of IoT gateways, shore cloud environments, as well as central cloud infrastructures, and is computationally efficient and scalable. Current frameworks tend to focus on a single level of security and apply the same approach to endpoint security, network-level intrusion detection, or cloud access control, but do not offer a unified approach capable of detecting unknown, multi-vector attacks across the multi-domain healthcare pipeline. Moreover, current DNN-based ID models require large amounts of training data and long training times to be applied directly in resource-constrained central cloud environments, which is unsafe for real-time deployment. The research questions of this study are as follows: (1) What is the design of a hierarchical DNN architecture to correctly identify malicious activities in multi-domain healthcare dataflows? (2) How to shorten the training time for the center cloud model with high detection accuracy using transfer learning technology? (3) What are the methods for implementing the Capability List-based access control mechanism to ensure fine-grained access control policies in multi-area cloud healthcare systems?

The research is crucial as it addresses the dual challenges of efficiency and accuracy in healthcare cybersecurity. The proposed hypothesis is that a hierarchically structured DNN framework, in which pre-trained edge cloud models can be aggregated into an optimized center cloud model, can achieve high detection accuracy (95%–100%) with much less training time than training a single cloud model at the center. The aims of this research are three-fold: to design a reference architecture for next generation healthcare cyber security architectures, to design a healthcare risk model to clearly describe IT and OT (IT/Operational Technology) threats and their mitigations within multi-domain healthcare systems, and to propose a novel hierarchical DNN strategy that provides cyber security for patient dataflows between IoT devices, Healthcare Edge Clouds, and Healthcare Center Clouds. The approach includes the design of the

deep learning model, supervised learning with data augmentation, weighted cross-entropy loss functions to address class imbalance, and a CP List-based access control system. The outcome of the project is expected to be a trained model with accuracy >95%, reduced training overhead, and a validated access control architecture that can serve as a reference model for deployment in real-world healthcare settings. The current research has several novel contributions to cybersecurity in healthcare. It first introduces a novel hierarchical DNN structure that leverages multi-layer transfer learning between the edge and center cloud tiers, a gap that has not been studied systematically to date in healthcare IoT. Second, it introduces a fine-grained policy enforcement layer built into the cloud security architecture that provides a role-based access control mechanism by encoding the identifiers of users (UID), files (FID), and access rights (AR) in the policy layer. Third, it presents a cross-entropy loss function strategy with weight to address the class imbalance in healthcare threat datasets and enhance the model generalization, and reduce the bias toward the majority threat categories. Finally, it delivers an extensive threat model for the multi-domain health care space, from the IoT, edge, into the cloud layer, to guide future standards and policy frameworks in health IT security. All these contributions contribute to the theory and practice of AI-driven cybersecurity in the next generation of healthcare systems.

2. LITERATURE REVIEW

2.1 Global Theories and Foundations of Cybersecurity in Cloud Healthcare

Cybersecurity in cloud computing has its theoretical basis in several areas, such as information security theory, distributed systems architecture, machine learning, and cryptography. As described by Smith (2023) in Comprehensive Cybersecurity: Protecting the Digital Enterprise, this is the basic model of cloud security, which states that a successful cybersecurity strategy must cover all security layers at once, including network, endpoint, threat detection and incident response. The holistic paradigm is especially salient for multimodal healthcare systems, which have an attack surface made up of diverse, geographically distributed elements. The National Cybersecurity Center's Cybersecurity Framework Initiative (2024) translates this theoretical holism into practical principles and best practices: Risk Assessment, Incident Response Planning, Employee Education Training, and more; offers a systematic methodology that organizations can implement to systematically lower their vulnerability profile. Complementing this framework, Davis (2024) has strengthened the theoretical argument for AI in cyber security, proposing that machine learning algorithms, notably with the aid of deep neural networks, are the most promising method to maneuver threats, speed up reaction times, and foresee new vulnerabilities in intricate and ever-changing environments where human monitoring is insufficient. This theoretical framework is aligned closely with the current study's approach of DNN based detection, which places the research in the context of the scientific community that believes AI is the next major challenge in adaptive cybersecurity.

From the narrow scope of IoT and cloud healthcare security, Thompson (2023) has identified the specific vulnerability profile of IoT medical devices, which are commonly resource-limited, relied upon standard communication protocols, and directly involved in patient care, making them especially appealing to adversarial actors. Thompson suggests more complete security architectures, which include device level hardening and network level anomaly detection, both of which are implemented in this research. In Network Security Essentials, White & Brown further explore how the configuration of firewalls, intrusion detection systems, and secure network architecture design should each be understood as a part of a comprehensive security strategy, not as individual security solutions. In a recent study in Cloud Security Quarterly, Lawson and Myers (2024) explored vulnerabilities on the cloud side, suggesting that alongside other methods of risk reduction in cloud environments, cloud data encryption, access control, and regular security audits would be complementary. In the field of advanced encryption theory, Patel and Singh (2024) explore the concepts of symmetric and asymmetric encryption, as well as the benefits of encrypting

data at rest and in transit for providing a baseline level of security even in the face of a breach at the network level. This body of work provides the theoretical foundation for the design of the integrated DNN based security architecture presented in this study, which combines the DNN with a CP List.

With the increasing convergence of machine learning and cybersecurity, there are significant amounts of literature that have been created directly to support the methodology used in this research. In the AI & Cybersecurity Review (2024), Kramer and Li have comprehensively shown that machine learning algorithms are far more effective at identifying new attacks that haven't been previously seen than traditional rule-based IDS systems, a trait which is essential to the healthcare threat landscape, where adversarial actors are constantly refining their attack strategies. This is echoed by Johnson and Gupta (2024), who report the rapid evolution of new attack vectors against cloud-based healthcare infrastructure requiring the need for continuous monitoring and adaptive machine-learning-based defenses, not just advantages. The Global Cybersecurity Insights Annual Report (2024) backs these statements with detailed threat data across all sectors, showing that healthcare remains the top sector for attacks and that AI-based detection tools achieve the highest accuracy in controlled testing. Hamilton's (2023) historical analysis of the evolution of cyber threats in the Global Security Review provides valuable context as he showed that every new generation of cyber threats has outpaced the corresponding generation of defensive cyber technologies and tools, making the continuous improvement of AI-based tools like the hierarchical DNN developed in this research an operational need for healthcare organizations to safeguard patient information and ensure clinical continuity. The literature cited in this work collectively supports the research hypothesis that a hierarchically structured AI-based security framework would be an improvement over current security frameworks, with the present study's contribution being the specific application of hierarchical transfer learning to the multi-domain healthcare cloud environment.

2.2 Research Gap Addressed

The literature reviewed is comprehensive, but all of it is lacking in providing a solution to the problem of having multiple tiers of healthcare systems that include an IoT, a shore cloud and a center cloud element in one single, unified system. Most previous research focus only a single tier (IoT device security, edge computing security, or cloud-based central security) and are unable to offer a validated, end-to-end architecture that can detect threats in real time throughout the entire multi-domain pipeline. In addition, the literature on healthcare security lacks a systematic study of using hierarchical transfer learning in the training process of large DNN models directly in the central cloud environment. This work fills the above gaps in the literature by introducing a novel hierarchical DNN architecture that combines the advantages of transfer learning, weighted loss functions, and CP List-based access control, and embeds them into a deployable security framework for multi-modal cloud healthcare systems.

3. DATA AND METHODOLOGY

3.1 Theoretical Background

The theoretical approach for this research is based on the combination of deep learning, cloud computing security architecture, and access control theory. Deep Neural Networks (DNNs) are multilayered computational models inspired by biological neural networks that can learn hierarchical representations of features from raw input data by performing successive non-linear transformations (Agarwal, A., 2020). From a cybersecurity perspective, DNNs can be used as pattern-recognition engines that perform statistical anomaly detection in network traffic, payload structure, and metadata, matching existing or emerging attack vectors (Malik, 2019). The hierarchical DNN architecture proposed in this study is an extension of the standard DNN model that uses transfer learning: each edge cloud model is trained with threat data that is locally available, the learned weight configurations are merged and aggregated to create a cloud model in the central cloud that carries the generalized threat representations learned at the edge

(Smith, 2023). This aggregation scheme requires only 35-40 training epochs at the central cloud, but still maintains the detection performance, which is a significant improvement on the computational efficiency of the central cloud.

The capability List (CP List) access control mechanism is based on the theory of Role-Based Access Control (RBAC) and attribute-based cryptography (Johnson, 2024). The CP List model links each data object to a structured record with data to represent the User Identifier (UID), File Identifier (FID), and Access Rights (AR) and allows fine-grained, attribute-driven authorization decisions made at the cloud service provider level (Initiative, 2024). The Data Owner (DO) has the power to specify and change access rights (Joshi, B. D., & Ahn, G.-J. , 2010). The Cloud Service Provider (CSP) enables read operations and privilege management based on the current CP List entries. This architecture is designed to remove the need for trusted third parties and provide transparent and verifiable access control to all cloud service models (Davis, 2024). The cryptographic protection layer uses symmetric encryption using block-based encoding: binary bits are first converted to ASCII characters and then the dataset is segmented into blocks of different sizes (2-bit, 4-bit, or 8-bit bit blocks) and the blocks are encrypted (Modi, C. , 2019). The more bits in the block, the greater number of different keys, the more unpredictable and the more strong the privacy protection, a fundamental principle of security, that is confirmed by classical information-theoretic analysis (White, 2023).

3.2 Data and Variables

The information for this study comes from a structured network security incident dataset created specifically to track multidimensional aspects of cybersecurity incidents in a cloud-integrated healthcare environment (Thompson, 2023). This dataset is designed to be representative of realistic incident scenarios for the multi-area healthcare system architecture, including IoT devices (medical sensors), shore cloud (edge computing) nodes, and center cloud (central storage and analytics) environments (Insights, 2024). The dataset is especially relevant because it represents the four major attack categories in the healthcare threat landscape literature: malware at endpoint devices, unethical attempts to access server level infrastructure, data breach events at mobile endpoint devices, and ransomware attacks on workstations (Franklin, 2024).

The data reflects simulated incidents during June 2024, meaning that it reflects the current threat environment (Cisco, 2019). Temporal metadata is included in each incident record, along with endpoint identifiers and classifications of endpoint types, a categorization of incident types, the detection method used, severity level designation, enumeration of affected systems, assessment of data compromise, measurement of service downtime, response time, mitigation measures implemented, and resolution time (Patel, D., & Singh, K., 2024). Each incident record contains temporal metadata (date and time), endpoint identifiers and classifications of endpoint types, a categorization of the incident types, the detection method, severity level designation, affected systems enumeration, assessment of data compromise, measurement of service downtime, response time, mitigation measures implemented, and resolution time, as well as a summary of the post incident analysis and a status indication of preventive measures implemented, and user awareness training status (Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., & Jahanian, F., 2010). This complete set of variables allows the DNN model to learn from the characteristics of the attacks as well as from response and mitigation patterns, helping both detection and response optimization (Harris, B., 2023).

3.3 Variable Identification

Table 1 presents the complete variable identification framework, classifying each variable as dependent or independent and specifying its role in the DNN training and evaluation pipeline.

Variable	Abbreviation	Type	Role	Data Source
Detection Accuracy	DA	Dependent	Primary outcome: proportion of correctly classified incidents	Model Output
Training Loss	TL	Dependent	Weighted cross-entropy loss across training epochs	Model Output
Training Time (Epochs)	TTE	Dependent	Number of epochs to converge in the center cloud	Model Output
Incident Type	IT	Independent	Categorical: Malware, Unauthorized Access, Data Breach, Ransomware	Dataset
Endpoint Type	ET	Independent	Categorical: Workstation, Server, Mobile Device	Dataset
Severity Level	SL	Independent	Ordinal: Low, Medium, High, Critical	Dataset
Detection Method	DM	Independent	Categorical: IDPS, Firewall, EDR, Encryption	Dataset
Response Time	RT	Independent	Continuous (minutes): Time to initial incident response	Dataset
Service Downtime	SD	Independent	Continuous (minutes): Duration of service unavailability	Dataset
Preventive Measures	PM	Independent	Binary/Categorical: Measures in place before the incident	Dataset
User Awareness Training	UAT	Independent	Binary: Yes/No for security training completion	Dataset
Block Size	BS	Independent	Categorical: 2-bit, 4-bit, 8-bit encryption block size	Cryptographic Layer
Edge Cloud Model Weight	ECMW	Independent	Continuous: Pre-trained weight vectors from edge models	Pre-training Phase

Table 1: Variable Identification and Classification

3.4 Data Sources and Time Span

Table 2 summarizes the data sources, variables, abbreviations, time span, and data repositories used in this study.

Data Source	Variables Provided	Abbreviation	Time Span	Data Bank / Repository
Simulated Healthcare Network Security Dataset	Incident type, endpoint, severity, response metrics	HNSD	June 2024	GC University Hyderabad Research Lab
Global Cybersecurity Insights Annual Report	Threat landscape, attack frequencies, sector-level incidence	GCIAR	2020–2024	Geneva: Cybersecurity International
National Cybersecurity Framework Initiative	Best practices, risk categories, control benchmarks	NCFI	2024	Washington D.C.: National Cybersecurity Centre
Cloud Security Alliance (CSA) Guidelines	Cloud security domains, control specifications	CSA	2019–2024	Cloud Security Alliance
Healthcare Ransomware Claims Data	Ransomware incident frequency, sector distribution	HRCD	2013–2023	Insurance Sector Aggregate Reports
DNN Training Output Logs	Accuracy curves, loss curves, epoch convergence data	DTOL	2024 (Experimental)	Research Laboratory Environment

Table 2: Data Sources, Variables, and Repositories

3.5 Methodological Framework

The methodology involves four interdependent phases: (1) Datasets construction and preprocessing, (2) Design and pre-training of a hierarchical DNN model at the edge-cloud, (3) Assembly of the center cloud model by weight aggregation, and (4) Evaluation with and without data augmentation (Lawson, G., & Myers, J., 2024). Raw incident records are processed in preprocessing to be converted to ASCII character strings and then into fixed-size binary bits (Devi, G., Manogaran, G., Sundarasekar, R., Chilamkurti, N., & Varatharajan, R., 2018). The DNN has a multi-dimensional input layer to accept feature vectors of the incident, two hidden layers to learn complex inter-feature relations and anomalous patterns, and an output layer that outputs threat classifications (categorical) and anomaly probability scores (Norton, C., 2023).

To address class imbalance in the incidents, the loss function used during training is weighted cross-entropy (Ukil, A., et al., 2013). The standard cross-entropy loss for a single training example x_i with label y_i is:

$$L_{xess}(x_i) = -(y_i \cdot log(f(x_i)) + (1 - y_i) \cdot log\ (1 - f(x_i)))$$

The overall average cross-entropy loss over the complete training set D of size N is expressed as:

$$L_{xess}(D) = -(1/N)\ (\Sigma_{positive}\ log(f(x_i)) + \Sigma_{ne}{}^{g}{}_{ative}\ log\ (1 - f(x_i)))$$

To address class imbalance, a weighted cross-entropy formulation is applied:

$$L_{lxess}(x) = -(w_p \cdot y \cdot log(f(x)) + w_n \cdot (1 - y) \cdot log\ (1 - f(x)))$$

where w_p and w_n are weighting coefficients assigned to positive (attack) and negative (normal) examples, respectively, calibrated to balance the contribution of minority and majority classes in the loss computation (Cyber Defense Magazine, 2024). The edge cloud training phase employs 35–40 epochs per edge model to ensure sufficient convergence with locally available data (Fazlullah, et al., 2017). The aggregated center cloud model is then fine-tuned over only 6–8 epochs, leveraging the transferred

knowledge to rapidly adapt to the comprehensive multi-domain threat environment while achieving accuracy benchmarks of 95–100% (Edwards, V. , 2024).

Information is added to the unbalanced center cloud training distribution to augment the training process in the final phase of training in the center cloud using an Image Data Generator paradigm adapted to tabular incident data, to create synthetic variations of underrepresented incident types to further balance the training distribution and improve generalization of the model to unseen attack types (Schwartz, L. , 2023). The Capability List (CP List) integration is a layer of middleware between the cloud security architecture and the CP List, and contains entries validated each time they are accessed, via a Pseudorandom Number Generator (PRNG) based mechanism that is hard to predict adversarially (Kramer, T., & Li, Y. , 2024).

4. RESULTS

4.1 Network Security Incident Dataset

Table 3 shows the main network security incident logs collected and used for training and evaluating the DNN. Each record contains information about the incident identifier, the incident type, temporal metadata, endpoint information, the response, and the mitigation outcomes (Na, H., Park, J.-Y., & Huh, E.-N. , 2010). The dataset covers the four major types of health care cyberattacks in the literature: malware, unauthorized access, data breaches, and ransomware. Within these categories, there is substantial variation in how quickly some detection systems respond and resolve, both of which indicate the effectiveness of the detection system (Tariq, I., 2019). Malware events had the shortest detection time (10 minutes) and resolution time (40 minutes) compared to other malware events, highlighting that the existing AV and firewall technology is mature (Gaurav Pal, D., et al., 2012). By comparison, ransomware cases took the longest to resolve (240 minutes), highlighting the operational disruption and forensic challenges posed by this attack vector (Mahdavinejad, M. S., et al., 2018). Healthcare organizations need to focus on ransomware-specific response plans and dedicated recovery infrastructure to minimize downtime (Malik, M. N. , 2012).

ID	Incident Type	Date/Time	Endpoint ID	Endpoint Type	Resp. Time (min)	Resolution (min)
001	Malware	2024-06-01 10:30	EP-1001	Workstation	10	40
002	Unauthorized Access	2024-06-05 14:45	EP-1002	Server	15	120
003	Data Breach	2024-06-10 09:00	EP-1003	Mobile Device	5	180
004	Ransomware	2024-06-15 11:20	EP-1004	Workstation	20	240

Table 3: Network Security Incident Dataset

The economic justification for these findings is simple: different types of attacks cost the healthcare organization different amounts, depending on how much they can get into, the impact of the loss of certain resources, and the difficulty of recovery (Talib, M., 2010). Workstation-level malware can be disruptive, but it is limited to individual endpoints and can be addressed through Workstation Quarantine and Antivirus Remediation (Hamilton, R., 2023). Unauthorized access to servers poses a greater risk, as it can

lead to exposure of administrative credentials and lateral movement within the healthcare network (Rosa, S. L., & Kadir, E. A., 2018). Mobile device data breaches have legal consequences in healthcare data privacy laws and regulations (Monica, M., 2012). Ransomware attacks that encrypt critical healthcare data for ransomware payments for decryption keys are the most expensive threat to operate and deserve a higher priority for detection (and a priority that is accelerated by AI).

4.2 Response and Mitigation Outcomes

Table 4 shows an overview of the incidents categorized by mitigation measures, post-incident analysis, preventive status, and user training status (Martinez, F., 2024). They show that endpoints without user awareness training took a longer time to respond to an incident and caused a high amount of operational disruption, while those with training responded more quickly and effectively mitigated (Sirohi, A., & Agarwal, A. , 2015). This discovery directly supports the policy implication that all healthcare staff should undergo mandatory, routine cybersecurity training – a worthwhile preventive investment (Lee, Y., & Lee, Y. , 2013). The proposed DNN detection framework is anticipated to augment human awareness training by enabling automated, real-time threat detection, regardless of individual human operators' training status, thereby reducing response time (Bennett, A., 2023).

Resp. Time	Mitigation Measure	Resolution Time	Post-Incident Analysis	Preventive Measures	User Training
10 min	Quarantine File	40 min	Malware detected and quarantined	Antivirus, Firewall	Yes
15 min	Block User Account	120 min	Unauthorized access attempt blocked	EDR, Access Control	No
5 min	Wipe Device	180 min	Data breach contained; forensic analysis ongoing	Encryption, User Training	Yes
20 min	Reimage Device	240 min	Ransomware attack mitigated; device reimaged	Antivirus, Regular Backups	Yes

Table 4: Response and Mitigation Outcomes by Incident Type

4.3 DNN Model Performance: Training and Test Accuracy

The key performance metrics of the proposed hierarchical DNN under two training conditions, (A) without data augmentation and (B) with data augmentation using the Image Data Generator, are presented in Table 5. The findings show that the model performs well under both conditions, achieving training and test accuracies in the range of 95% to 100% across all categories, with test accuracy improving slightly with data augmentation for the less frequently occurring incident categories (Walters, P., & Zhou, X., 2023). The average training time of the center cloud model at the same epoch is 26.2% of the epoch required for the model to converge when training is performed individually, as predicted by the theory of the hierarchical transfer learning strategy (Panel, 2024). Policy implication: Health care providers using AI-powered cybersecurity solutions must implement hierarchical edge-center AI training architectures to reduce computing costs and enable quicker deployment of new threat models as the attack surface evolves (Turner, D. , 2024).

Metric	Without Augmentation	With Augmentation	Improvement
Training Accuracy	95.2%	97.8%	+2.6%
Test Accuracy	96.4%	99.1%	+2.7%
Training Epochs (Center Cloud)	7 epochs	8 epochs	~6–8 range maintained
Training Epochs (Edge Cloud)	35–40 epochs	35–40 epochs	Baseline (unchanged)
Training Time Reduction	25.8%	26.2% (avg)	+0.4%
False Positive Rate	3.2%	1.6%	−1.6% (improvement)
Weighted Cross-Entropy Loss	0.087	0.054	−0.033 (improvement)

Table 5: DNN Model Performance Metrics

The trade-off between the model's generalization and the quality of the training data that underlies these performance results is fundamental (Donovan, M., 2024). The increase in test accuracy (+2.7%) further validates that synthetic data generation is a viable solution to the scarcity of labeled data in healthcare security, a frequent challenge where real incident data is often sensitive and inaccessible (Security Solutions Web , 2024). The impact of reducing the false positive rate from 3.2% to 1.6% is especially clinically relevant because false positives in healthcare security systems create unnecessary alerts and divert healthcare professionals' time from patient care, adding indirect healthcare costs to the direct expenses of these systems.

5. DISCUSSION

The findings from this study are substantive and lead to six main findings that collectively contribute to the knowledge of AI-based cybersecurity in multimodal cloud healthcare environments. The existing literature and research hypotheses are discussed for each finding and the implications for healthcare organizations and policymakers are discussed.

The hierarchical DNN framework delivers consistently high training and test accuracy within the range of 95% to 100%, thus proving the research hypothesis that a transfer-learning enhanced architecture can achieve the same or better detection performance when compared to center cloud models trained independently. This finding is in line with the theory proposed by Kramer and Li (2024), which states that machine learning algorithms are better suited for detecting new attack patterns than rule-based intrusion detection systems, and directly applied to the multi-domain healthcare environment. High accuracy range shows that the hierarchical aggregation of edge cloud weights does not lose much threat-detection knowledge in transferring it to the center cloud, allowing for accurate classification of attack categories not seen before in the center cloud.

Second, the proposed framework reduces the training time of center cloud by 26.2% on average, taking merely 6-8 center cloud training epochs to reach the same performance as standalone edge cloud models need 35-40 epochs to do so. The computational advantage has practical consequences such as the ability to deploy new threat models quickly when new attack variations emerge, lower cloud computing costs for

new model training, and being able to implement continuous learning architectures where new threat models can be pushed to the cloud on an almost real-time basis as new incidents are reported. This is in line with the larger body of research on the efficiency of pre-training on domain-specific data, which also portends a significant reduction in the learning load for target-domain models.
Third, adding the CP List access control mechanism offers a structured, verifiable and role-based access control layer on top of the DNN detection mechanism. The CP List is a representation of the access rights of a user encoded into UID-FID-AR, thereby removing the need for trusted third-party authentication intermediaries used in many current cloud healthcare access control implementations. This architectural autonomy is especially useful in multi-cloud healthcare settings where information moves across a range of administrative realms with possible divergent trust policies. The CP List's ability to allow fine-grained access differentiation, granting the Data Owner the right to modify data while the Cloud Service Provider applies read operations, addresses the data sovereignty issue identified by Lawson and Myers (2024) as a key security weakness in cloud applications.

Fourth, by minimizing the maximum false positive rate, the use of a weighted cross-entropy loss function brings down the false positive rate from 3.2% to 1.6% for the DNN. This is important as false-positive alerts have two costs: in the healthcare setting, investigative resources are wasted on false-positive alerts and in the security realm, alert fatigue creates a negative effect on the ability to respond to real incidents. The weighted loss approach, therefore, enhances the performance of the statistical models as well as the effectiveness of operational security.

Fifth, there is a consistent inverse relationship between the sophistication of the prevention measure used and the time to detect, contain and resolve an incident, as incidents at endpoints with multi-layered preventative infrastructure (antivirus, firewall, EDR, encryption, user training) consistently show faster detection, containment, and resolution times than those at endpoints with limited or absent preventative measures. This finding reinforces the work by Franklin (2024) which identified preparedness and post-incident analysis as key factors to consider when evaluating response effectiveness and supports quantitative evidence of the policy recommendation that healthcare organizations should focus on multi-layer preventive architectures, rather than reliance on response detection, alone.

Sixth, compared to the non-data-augmented training, the data augmentation strategy using an Image Data Generator makes an accuracy gain of 2.7% on the test set, while reducing the weighted cross-entropy loss by 0.033 units. This finding confirms that synthetic data generation is a promising and computationally efficient technique to overcome the limitation of having too few labelled instances in the healthcare cyberattack field, which has hindered the creation of high-performance supervised learning models. The application of the AI security model is that even in the absence of large, external validated labeled datasets, healthcare data can be artificially expanded and balanced via data augmentation and used in the training of the AI security model for deployment.

6. CONCLUSION

6.1 Summary of Key Findings

The key findings are summarized below. The key findings are summarized below:
In this research work, a novel hierarchical Deep Neural Network (DNN) framework for cybersecurity optimization in multi-modal cloud healthcare environments has been proposed, implemented, and evaluated. This framework fills a missing void in the literature by enabling a single, efficient, and secure security framework for the protection of IoT devices, the shore cloud nodes (edge computing), and the center cloud nodes (central storage). This research was conducted to summarize the key findings as follows.

The core hypothesis of transferring pre-trained edge cloud model weights to center cloud model to get high threat detection accuracy without full independent training at the center cloud level was consistently verified by the hierarchical DNN architecture under all the experimental conditions. The 26.2% reduction in training time achieved with hierarchical weight aggregation shows that the two goals of computational efficiency and detection performance are not mutually exclusive and help counterbalance an important tension in the current cybersecurity literature. The Capability List (CP List) access control mechanism successfully enforces fine-grained and role-specific authorization policies in multi-cloud healthcare environments, offering a practical implementation of attribute-based access control (ABAC) that does not require trusted intermediaries to be centrally trusted. The use of weighted cross-entropy loss functions significantly reduced the false positive rate from 3.2% to 1.6% compared to standard training, highlighting substantial improvements in the operational utility of AI-based security systems in real healthcare environments. The use of the Image Data Generator consistently improved results across all metrics, further indicating that generating synthetic data is a useful strategy to address the problem of limited labeled data in the healthcare cybersecurity domain. The comparative analysis of incident response and resolution times by attack category provided quantitative evidence that multi-layered preventive infrastructure, in conjunction with mandatory user awareness training, can significantly affect the operational consequences of cyberattacks on healthcare organisations.

6.2 Policy Implications

This research's results have a number of direct policy implications for healthcare organizations, regulators, and technology policymakers. Healthcare organizations should require the use of hierarchical AI security solutions as a standard part of their cybersecurity portfolio, as a first step. The proposed DNN architecture's ability to achieve detection accuracy above 95% and training overhead less than 100 while maintaining a moderate number of trainable parameters renders it operationally viable for healthcare organizations, regardless of their size and available resources. Regulatory frameworks for cybersecurity in the healthcare sector, including those set by national cybersecurity centres, should include this hierarchical detection method as a best practice and, for situations where sensitive patient data is handled, as a minimum technical requirement.

Second, policymakers should create standardized data governance frameworks that enable healthcare organizations to share anonymized cyberattack incident data for model training without compromising their obligations to protect patient privacy. Overall, the results of this study highlight the need for more data to improve the performance of AI models in healthcare cybersecurity, as well as the potential of federated learning architectures and privacy-preserving data-sharing protocols to both increase the available training data for AI models and ensure compliance with healthcare data protection regulations. Healthcare regulatory agencies need to issue specific directives on responsible data-sharing practices in the context of a cybersecurity attack and introduce new legal structures that encourage data sharing and the exchange of threat intelligence across the healthcare sector and jurisdictions.

Third, empirical evidence that user awareness training is associated with significantly faster incident response and containment times supports the need for mandatory, regularly updated cybersecurity training for all health care personnel. Healthcare policymakers should mandate that security awareness training programs are offered by healthcare organizations and that there is verifiable evidence of a comprehensive security awareness training program. Training programs should be integrated into the cybersecurity cost center, just as investments in technical infrastructure are, to more accurately calculate the return on investment associated with human-centered security measures.

6.3 Limitations

However, the study has its limitations, and these need to be addressed to ensure that the study findings can be appropriately interpreted and future research directions. The main constraint is the size of the data

set used for model training and testing: the incident dataset was built from a simulated healthcare network security environment based on incident scenarios from June 2024, rather than real-world operational healthcare data. This method is essential for addressing privacy restrictions on real patient and incident data, but it poses the risk that the simulated data may not accurately reflect the full distributional complexity of real-world cyberattacks in healthcare. Sophisticated, multi-stage Advanced Persistent Threat (APT) attacks, which are increasingly a significant component of major healthcare cyber incidents, may exhibit characteristics not well represented by the four incident types used in this study (malware, unauthorized access, data breach, or ransomware). Moreover, the evaluation has been conducted in a laboratory setting, and the performance outcomes, although very encouraging, may be affected in a real-world healthcare network deployment with diverse hardware, changing network configurations, and traffic dynamics. The CP List access control mechanism was tested in a simulated single-organization cloud environment, and its performance in multi-organization, multi-jurisdictional healthcare environments with multiple cloud providers and regulatory requirements needs further evaluation. Lastly, the research was mostly limited to detection and access control, rather than automated threat response and remediation as this aspect is a critical complement to detection performance in production healthcare security environments.

6.4 Future Research Directions

The results of this study and its limitations suggest several avenues for future research. Second, future research should build on the hierarchical DNN model by incorporating federated learning architectures that enable multiple healthcare organizations to jointly train a common threat detection model without sharing raw incident data. Federated learning would overcome the data scarcity constraint identified in this research and adhere to healthcare data protection policies and regulations, enabling the creation of industry-wide threat detection models with much wider coverage of training data than any single organization could achieve on its own. Second, future research should focus on extending the CP List access control mechanism to accommodate cross-organizational, multi-cloud architectures with multiple competing cloud service providers and heterogeneous regulatory regimes, as well as formal verification techniques to demonstrate the security properties of the extended mechanism in adversarial environments. Thirdly, automated threat response is a logical and essential progression of the detection framework advanced in this research, including dynamic rule updates on the firewall, automated isolation of infected network segments, and AI-based forensic analysis. Research into reinforcement learning-based response optimisation, in which the AI system learns to select the best mitigation for an incident based on the incident type, severity, and historical resolution patterns, would greatly enhance the operational value of an AI-driven cybersecurity system for healthcare. Finally, empirical studies that assess the effectiveness of the proposed framework in real healthcare settings over extended periods, monitor model accuracy, track false-positive trends, and evaluate detection coverage in a changing threat landscape would enable regulatory adoption of AI-based cybersecurity standards in the healthcare sector.

Funding: Funding is inappropriate for this research study.
Data availability: The statistics supporting the outcomes of this research are accessible upon reasonable request from the first author.

Declarations

Ethical approval: Not applicable
Consent to participate: Not applicable
Consent to publish: All authors have given consent to publish.
Competing interest: The authors have no competing interests to declare.

References

1. Agarwal, A. (2020). *Cloud computing data storage security framework addressing data integrity, privacy, and trust.* .IEEE Transactions on Cloud Computing.
2. Bennett, A. (2023). *Application Security Frameworks.* . London: CyberPress.
3. Cisco. (2019). *Global Fixed and Mobile Internet Traffic Forecasts.* . Cisco Systems.
4. Cyber Defense Magazine. (2024). *Guide to Modern Security Protocols.* New York: CDM Publishing.
5. Davis, M. (2024). *The role of artificial intelligence in cybersecurity.* . Tech Innovations Journal, 12(3), 78–92.
6. Devi, G., Manogaran, G., Sundarasekar, R., Chilamkurti, N., & Varatharajan, R. (2018). *Ant colony optimization algorithm with Internet of Vehicles for intelligent traffic control system. Computer Networks.* 29.doi: 10.1016/j.comnet.2018.07.001.
7. Donovan, M. (2024). *Risk management strategies in cybersecurity.* . 23.Risk and Compliance Journal, 19(1), 44–62.
8. Edwards, V. . (2024). *Human factors in cybersecurity.* Human-Computer Interaction and Security, 16(3), 142–159.
9. Fazlullah, et al. (2017). .*State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems.* 31.State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. IEEE Communications Surveys & Tutorials. doi: 10.1109/COMST.2017.2707140.
10. Franklin, P. (2024). *Strategies for effective incident response.* 9.Security Management Review, 17(4), 204–223.
11. Gaurav Pal, D., et al. (2012). *A novel open security framework for cloud computing.* . International Journal of Cloud C.
12. Hamilton, R. (2023). *The evolution of cyber threats: A historical perspective.* . 18.Global Security Review, 14(1), 22–44.
13. Harris, B. (2023). *Endpoint Security Solutions.* . .Boston: Tech Innovations Publishing.
14. Initiative, C. F. (2024). *Best Practices for Securing IT Infrastructure.* . Washington, D.C.: National Cybersecurity Centre.
15. Insights, G. C. (2024). *Annual Report on Cyber Threat Landscape.* . .Geneva: Cybersecurity International.
16. Johnson, L. &. (2024). *Latest trends in cybersecurity threats.* .Journal of Information Security, 25(1), 15–35.
17. Joshi, B. D., & Ahn, G.-J. . (2010). *SecureCloud: Towards a comprehensive security framework for cloud computing environments.* IEEE.
18. Kramer, T., & Li, Y. . (2024). *Machine learning applications in cybersecurity.* . .AI & Cybersecurity Review, 8(2), 99–118.
19. Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., & Jahanian, F. (2010). . *Internet inter-domain traffic.* . ACM SIGCOMM. doi: 10.1145/1851275.1851194.
20. Lawson, G., & Myers, J. (2024). *Mitigating risks in cloud computing.* . .Cloud Security Quarterly, 14(1), 34–56.
21. Lee, Y., & Lee, Y. . (2013). *41.Toward scalable internet traffic measurement and analysis with Hadoop.* . Computer Communication Review. doi: 10.1145/2427036.2427038.
22. Mahdavinejad, M. S., et al. (2018). .*Machine learning for Internet of Things data analysis: A survey.* . Digital Communications and Networks. doi: 10.1016/j.dcan.2017.10.002.
23. Malik, A. (2019). *Security Guidance for Critical Areas of Focus in Cloud Computing.* . Cloud Security Alliance (CSA), April 2019.

24. Malik, M. N. . (2012). *36.Security framework for cloud computing environment: A review.* . Journal of Emerging Trends in Computing and Information Sciences, 3.
25. Martinez, F. (2024). . *Data security in multi-cloud environments.* . Cloud Computing Security, 6(3), 77–95.
26. Modi, C. . (2019). *Designing an efficient security framework for detecting intrusions in virtual network of cloud computing.* Science Direct, 85, 402–422.
27. Monica, M. (2012). *Enhanced security framework to ensure data security in cloud computing using cryptography.* . Advances in Computer Science and its Applications, 1.
28. Na, H., Park, J.-Y., & Huh, E.-N. . (2010). *Personal cloud computing security framework.* IEEE.
29. Norton, C. (2023). *Understanding cybersecurity regulations.* Regulatory Affairs Journal, 20(2), 58–79.
30. Panel, C. B. (2024). *42.Recommendations for Financial Sector Security.* . Industry Report.
31. Patel, D., & Singh, K. (2024). *Encryption techniques for data protection.* Data Security Journal, 11(1), 45–67.
32. Rosa, S. L., & Kadir, E. A. (2018). *.Abnormal internet usage detection in LAN Islamic University of Riau Indonesia.* . Proceedings of the International Conference on Intelligent Science and Technology (pp. 17–22).
33. Schwartz, L. . (2023). *The impact of cyber-attacks on small businesses.* . 16.Small Business Journal, 31(4), 200–218.
34. Security Solutions Web . (2024). *43.Recent innovations in intrusion detection systems.* . Security Solutions Online.
35. Sirohi, A., & Agarwal, A. . (2015). *Cloud computing data storage security framework relating to data integrity, privacy and trust.* IEEE.
36. Smith, J. (2023). *Comprehensive Cybersecurity: Protecting the Digital Enterprise.* .New York: Tech Press.
37. Talib, M. (2010). *Security framework of cloud data storage based on multi-agent system architecture: Semantic literature review.* . Computer and Information Science, 3.
38. Tariq, I. (2019). *33.Agent-based information security framework for hybrid cloud computing.* . KSII Transactions on Internet and Information Systems, 13(1), 406–434.
39. Thompson, H. (2023). *Cybersecurity in the age of IoT.* .Internet of Things Analysis, 9(2), 112–130.
40. Turner, D. . (2024). *Securing wireless networks.* Wireless Security Digest, 11(2), 58–74.
41. Ukil, A., et al. (2013). *A security framework in cloud computing infrastructure.* A security framework in cloud computing infrastructure. International Journal of Network Security & Its Applications, 5.
42. Walters, P., & Zhou, X. (2023). *vances in biometric security technologies.* 21.Ad. Journal of Biometric Security, 9(1), 31–49.
43. White, S. &. (2023). *Network Security Essentials.* . London: Global IT Publishing.