Informing Science:
the International Journal of
an Emerging Transdiscipline

An Official Publication
of the Informing Science Institute
InformingScience.org

Inform.nu

Volume 28, 2025

ADVERSARIAL ATTACKS ON HEALTHCARE DEEP LEARNING MODEL: VULNERABILITIES AND DEFENSES

Mekala A*	Department of Computer Science, Sacred Heart College, Tirupattur, Tamilnadu, India	mekalaresearch@gmail.com
Shahnaz Fatima	ECE Department, Sasi Institute of Technology & Engineering, Tadepalligudem, Andhra Pradesh, India	Shahnaz1981fat@gmail.com
Subba Rao BV	Department of IT, PVP Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India	bvsrau@gmail.com
Rajendra Prasad J	Department of IT, NRI Institute of Technology, Agiripalli, Vijayawada, Andhra Pradesh, India	rp.rajendra@rediffmail.com
Banupriya P.G	Karpagam Institute of Technology, Coimbatore, Tamilnadu, India	banupriya.cse@karpagamtech.ac.in
Venkata Ramana K	Department of CSE, QIS College of Engineering and Technology, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India	ramanakaveripakam@gmail.com

* Corresponding author

ABSTRACT

Aim/Purpose	The aim of this work is to introduce a novel technique for enhancing hospital network security using a Deep Autoencoder (DAE).
Background	The digitization of healthcare institutions increases the risk of cybercrime due to network security vulnerabilities.

Accepting Editor Eli Cohen | Received: October 19, 2024 | Revised: January 30, 2025 | Accepted: January 31, 2025.
Cite as: Mekala, A., Fatima, S., Subba Rao, BV., Rajendra Prasad, J., Banupriya, P.G., & Venkata Ramana, K. (2025). Adversarial attacks on healthcare deep learning model: Vulnerabilities and defenses. *Informing Science: The International Journal of an Emerging Transdiscipline, 28,* Article 7.
https://doi.org/10.28945/5452

Methodology	In this work, we model a novel technique called DeepHeal framework that uses a robust Deep Autoencoder (DAE) for improved cybersecurity and protection against intruders in healthcare networks. Using the deep learning techniques named DAE, DeepHeal identifies and stops cyber dangers, including various hostile attacks, illegal access, and data breaches. Healthcare networks are susceptible to various cyberattacks and intrusions. The DAE architecture enables training with high-level representations to detect anomalies and traffic patterns. By carefully analyzing datasets from real healthcare networks, we demonstrate that DeepHeal effectively identifies and counters various cyber threats.
Findings	The proposed DAE model combined with RNN achieves a higher accuracy and precision level of 98%. The proposed DAE model outperformed existing models, which offers its ability to identify and resolve cybersecurity problems in hospital networks.
Future Research	The proposed method's research offers great potential in terms of accuracy, scalability, and real-time threat detection.

Keywords network security, DAE, DHeal, healthcare

INTRODUCTION

This study is a detailed exploration of the increasing digitalization of healthcare networks and the current state of healthcare IT systems, including the widespread use of electronic health records (EHRs), medical IoT devices, and telemedicine. Furthermore, providing an overview of traditional cybersecurity measures, like signature-based and rule-based Intrusion Detection Systems (IDS), will help readers understand the limitations of these approaches. Comparing these existing systems with the potential of Deep Autoencoders (DAE) in anomaly detection can set the stage for why DAE-based solutions are a promising alternative.

The digital transformation in healthcare has significantly advanced the management and delivery of services. Networked medical devices, telemedicine, and electronic health records (EHRs) have enhanced healthcare efficiency and accessibility (Puttagunta et al., 2023).

This digital revolution leads to increased threats and vulnerabilities, where threats to healthcare networks are common, including malware, data breaches, ransomware, and illegal access. These risks to patients' private data affect the dependability and availability of healthcare services (Veerappan et al., 2023).

The COVID-19 epidemic has brought the critical need for network security in healthcare facilities. The attack surface is considerably growing with the development of remote healthcare and telemedicine delivery techniques. Therefore, the probability of cyberattacks in the healthcare system is increased. Modern security solutions and cybersecurity procedures are invested in healthcare businesses to secure these systems and data of patients against cyber threats (Ahuja et al., 2024).

The likelihood of illegal access and breaches increased due to the increasing digitization of healthcare systems, prompting people to express concerns about the privacy and security of healthcare patient data. Cybersecurity is a serious issue in the healthcare industry as intruders attempt to exploit network security to get sensitive patient data, which may include invasion of privacy, medical treatment disruption, and patient damage (Kaviani et al., 2022).

This work aims to introduce a novel technique for enhancing hospital network security using a Deep Autoencoder (DAE). DAE is being used to prevent cyberattacks by early identification and mitigation. The research aims to involve network integrity and data protection against sensitive patients.

The findings of this paper increase hospital network security in several ways. An upgrade that is much needed is the DAE-enabled approach for hospital cybersecurity. Since the Intrusion Detection System (IDS) may identify odd network behavior in real-time following DAE integration, healthcare networks may be better safeguarded against intrusions.

Deep learning methods have been improved by research and are a part of the cybersecurity framework. The viability of unsupervised learning for the purpose of identifying anomalies and cyber dangers in healthcare networks is evaluated in this work using DAEs. This paper demonstrates the effectiveness of deep learning in protecting cybersecurity threats in the healthcare industry, extending its use outside of traditional domains.

The proposed method provides a thorough and practical solution for healthcare companies to enhance their network security measures. The novelty of this work lies in the integration of Deep Autoencoders (DAE) for real-time intrusion detection and mitigation within healthcare network security.

RELATED WORKS

This study examines healthcare institutions' specific challenges in maintaining network security and protecting patient data (Saravanan, Parameshachari et al., 2023). This research on the continually changing threat landscape (Yuvaraj et al., 2022) encompasses a wide range of attacks, including malware infections, ransomware occurrences, and insider threats, to mention but a few of the many distinct forms of attacks that exist.

We go into the cybersecurity problems that healthcare facilities encountered in Costa et al. (2024). The numerous factors that make the healthcare sector open to cyberattacks are examined in this research (Saravanan, Sankaradass et al., 2023). The content of the literature review (Maguluri et al., 2023) suggests that cybersecurity incidents in the medical field can have serious consequences – included are the ethical and social ramifications of data breaches and their impact on patients' trust in medical practitioners (Rahman et al., 2020).

Our research on applying deep learning techniques in cybersecurity lays the groundwork for the next study (Zhang et al., 2022). It covers pertinent and uses research on anomalies, intrusions, and threats in several domains (Selvaganapathy & Sadasivam, 2021). The advantages of deep learning are mainly emphasized (Newaz et al., 2020). Moreover, in relation to cybersecurity are the advantages and disadvantages of deep learning architectures, such as autoencoders, recurrent neural networks (RNNs) and convolutional neural networks (CNNs) (Bortsova et al., 2021), high-dimensional data compatibility, and lack of supervision (Liu et al., 2021).

The focus of the analysis of the different methods and solutions already in use is network security for healthcare organizations. The paper analyzes the benefits and drawbacks of several approaches to show the necessity of developing creative and preventive cybersecurity solutions that can efficiently manage the constantly changing threat environment in the healthcare sector (Ma et al., 2021).

DAEs were chosen for anomaly detection due to their ability to efficiently handle high-dimensional, unsupervised data, which is common in healthcare network traffic. Due to their valuable patient data, healthcare networks are increasingly targeted by cyberattacks like ransomware, data breaches, and malware.

PROPOSED METHOD

The cybersecurity-based intrusion detection system (IDS) (Figure 1) proposed in the DeepHeal aims to improve security in healthcare networks via real-time threat mitigation and detection.

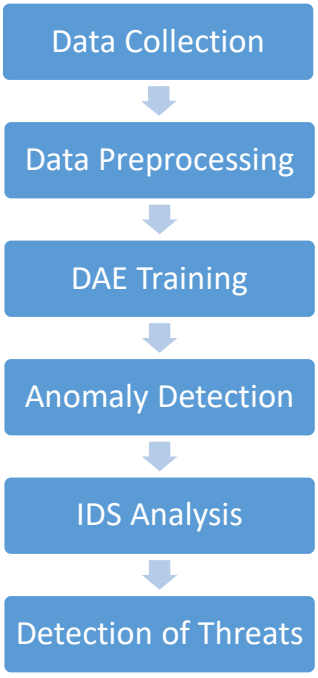

Figure 1. Process flow of the proposed IDS

Data Collection and Preprocessing

Data preprocessing steps, including noise removal, feature normalization, and handling missing values, were applied to ensure high-quality, consistent input for the model. This preparation enabled effective training and reliable anomaly detection. Specifically, the steps taken to remove noise and handle missing values should be clearly outlined, including the methods or algorithms used for imputation or data cleaning.

A substantial dataset reflecting real healthcare network activity is essential for training and evaluating the DeepHeal model. For the DeepHeal framework to train and assess the DAE model, high-quality data is necessary.

Data collection

In this section, we select and pinpoint the sources of the traffic on the healthcare network.

Data preprocessing

Remove Noise: Network traffic data analysis is not always accurate since the data has background noise, useless information, and artifacts.

Normalize Features: One way to ensure the network traffic's features are all on the same scale is to normalize them.

Handle Missing Values: Training with a dataset, including instances of missing values, requires handling missing values appropriately.

DAE

The DeepHeal framework heavily depends on the DAE architecture and training via gradient descent and backpropagation, allowing the DAE parameters to be refined. Reducing error during reconstruction aims to teach the autoencoder to detect abnormalities that could indicate possible cyber threats and precisely replicate standard network traffic patterns.

Table 1. DAE specifications

Component	Layer type	Number of units	Activation function
Encoder	Input Layer	1000	-
	Dense Layer 1	512	ReLU
	Dense Layer 2	256	ReLU
	Dense Layer 3	128	ReLU
	Bottleneck Layer	64	ReLU
Decoder	Dense Layer 1	128	ReLU
	Dense Layer 2	256	ReLU
	Dense Layer 3	512	ReLU
	Output Layer	1000	Sigmoid

ALGORITHM: DHEAL FRAMEWORK

- Initialize the weights and biases of the Denoising Autoencoder (DAE).
- For each epoch in the training process and each training sample in the dataset:
  - Pass the training sample through the encoder to get the encoded output.
  - Pass the encoded output through the decoder to get the reconstructed output.
  - Compute the reconstruction error by comparing the training sample and the reconstructed output.
  - Backpropagate the reconstruction error through the network.
  - Update the weights and biases based on the backpropagated error.
- For each new network traffic sample:
  - Pass the new sample through the encoder to get the encoded output.
  - Pass the encoded output through the decoder to get the reconstructed output.
- Compute the reconstruction error by comparing the new sample and the reconstructed output.
- If the reconstruction error exceeds a predefined threshold:
  - Use the Intrusion Detection System (IDS) to analyze the anomaly.
  - If the IDS detects a threat, perform mitigation actions to counteract the threat.
- Set up secure communication channels.

Ensure the DHeal framework works seamlessly with existing cybersecurity systems.

Encoder

The encoder reduces the dimensionality of the input data in an iterative manner to extract the most pertinent features. Several hidden layers comprise it, with convolutional layers or fully connected layers being the most frequent ways to apply them when working with data. Following the linear transformation of each layer is a non-linear activation function. The output of the encoder is the encoded representation, which is different from the latent space representation.

This is a list of the mathematical equations that describe the encoder:

$$\text{Encoder Output} = f(W_e * I + b_e)$$

where

I - input data
W_e - encoder weights
b_e - encoder biases
f() - activation function

Decoder

Following the receipt of the encoded representation, the decoder makes use of it to restore the initial data that was entered beforehand. Within its many hidden layers, both the encoder and the decoder make use of a combination of fully linked and convolutional layers. The objective of the decoder layers is to gradually raise the dimensionality in order to recover the data that was first entered. In most cases, the last layer makes use of an activation function that pertains to the characteristics of the data that is being input. For example, sigmoid functions are utilized for binary data, while linear functions are utilized for continuous data.

For convenience, the decoder employs the following mathematical formulas:

$$O = f(W_d * E + b_d)$$

where

E - encoded representation from the encoder
W_d - decoder weights
b_d - decoder biases
f() - activation function

Loss function

The goal of DAE learning is to reduce a loss function that evaluates the degree of dissimilarity between the input data and the rebuilt output. Mean squared error (MSE) is the loss function in continuous data, and binary cross-entropy is the loss function in binary data. The aim of the loss function is less space between the original input and the rebuilt output.

Among the loss functions used in DAE designs for continuous data, the Mean Squared Error (MSE) is the most frequent. The average squared difference is computed using the rebuilt output and the original input as inputs. When seen mathematically, the MSE loss function resembles:

$$MSE = n^{-1} * \sum(I - D)^2$$

where

n - training samples
Input - original input data
D - reconstructed output

Utilizing the number of training samples as input, the mean squared error (MSE) loss function divides the total number of elements by the squared difference between each input element and the reconstructed output. The parameters are given in Table 2.

Anomaly Detection

Here, we describe how to compute the reconstruction error following a network data sample feeding into a trained autoencoder. Samples with large reconstruction errors are instances of anomalies that may indicate the existence of potential cyber threats. Should anomalies be discovered, the intrusion detection system (IDS) of the DeepHeal framework begins additional research. Rule-based and signature-based detection methods are applied in this analysis to determine the type of threat and initiate appropriate actions.

The cybersecurity-based IDS in the DeepHeal architecture mostly gets its intelligence from anomalies. Finding the reasons why the network traffic statistics deviate from the norm can indicate the presence of malicious people or cyber threats.

With its analysis of normal network traffic patterns, the DAE can identify anomalies and outliers. The autoencoder, an encoder, and a decoder merged into one device duplicate entered data. We compare the reconstruction of the original data with it to get the MSE, or anomaly score. A stronger link between the MSE and the likelihood of an anomaly forming exists when the MSE surpasses the difference between the input data and the reconstruction.

Table 2. Parameters of DAE

Parameter	Value
Latent Space Dimension	32
Number of Hidden Layers	4
Number of Neurons per Layer	[512, 256, 128, 64]
Activation Function	ReLU
Loss Function	Mean Squared Error
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Number of Epochs	100
Dropout Rate	0.2
Weight Initialization Method	He Initialization
Early Stopping Patience	10
L1 Regularization Coefficient	0.01
L2 Regularization Coefficient	0.01
Learning Rate Scheduler	ReduceLROnPlateau
Data Normalization Method	Min-Max Scaling
Noise Injection in Input	0.1 (10% noise)
Batch Normalization	Yes
Validation Split	0.2 (20% validation data)

RESULTS

This closely examines the outcomes of our cybersecurity solution for the healthcare industry, which includes deep autoencoders enabled. The results illustrate how effectively the technology protects networks and identifies potential threats to the network. In addition, we discuss the implications of the data for healthcare organizations and the value of the data for those organizations.

DATASET

During our experiment, we used a representative network traffic dataset from a healthcare organization (Hussain et al., 2021).

The dataset used for training the DAE model was carefully selected and processed to ensure it accurately represented real-world healthcare network traffic.

- *Accuracy:* The proportion of correctly classified instances (normal and anomalous) out of the total number of instances.
- *Precision:* The proportion of correctly identified positive instances (true positives) out of all instances predicted as positive.
- *Recall (Sensitivity):* The proportion of correctly identified positive instances (true positives) out of all positive instances.
- *F1-Score:* The harmonic mean of precision and recall, balancing the two.

- *False Positive Rate (FPR):* The proportion of normal instances incorrectly classified as anomalies.
- *True Negative Rate (TNR):* The proportion of correctly classified normal instances.

We were successful in establishing a controlled laboratory environment that was able to simulate the network infrastructure of a hospital, as demonstrated in Table 3. There were components of the infrastructure that included network equipment characteristic of healthcare companies. These components included routers, switches, and firewalls. The architecture drew on the complexity and characteristics of actual healthcare networks. These features included virtual local area networks (VLANs), a wide range of traffic patterns, and numerous subnetworks.

Table 3. Dataset

Source IP	Destination IP	Packet size	Port	Label
xx.xx.0.1	xx.xx.1.20	1024	80	Normal
xx.xx.2.15	xx.xx.0.5	512	53	Normal
xx.xx.1.100	xx.xx.0.2	768	22	Anomalous
xx.xx.0.3	xx.xx.1.50	2048	445	Anomalous
xx.xx.1.10	192.168.0.4	4096	443	Normal
xx.xx.0.2	xx.xx.1.30	1536	3389	Normal

We searched the network traffic data for anomalies using a deep autoencoder design. PyTorch is a neural network framework used in model construction. One layer in the design, fully connected neural networks, compressed the input data. The data reconstruction was left to the next layer.

Experimental Metrics

Within the parameters of our study, we evaluated the system's effectiveness using various measures. Measures taken into account included the actual positive rate, the false positive rate, the overall detection accuracy, the actual negative rate, and the actual negative rate. Subsequently, we calculated the F1-score, recall, and precision to evaluate the system's anomaly detection performance against earlier methods like RNN and DAE. Our aim was to reduce false positive and false negative counts.

The experimental evaluation shows promising performance in Figures 2-5 and Tables 4 and 5 of the proposed DAE model for cybersecurity-based intrusion detection in healthcare. The proposed DAE model was able to identify between normal and pathological network traffic with an accuracy rate of 98% when operating with a maximum dataset size of 100 samples. Moreover, the accuracy values for the proposed DAE model were continuously high and varied from 89% to 97%.

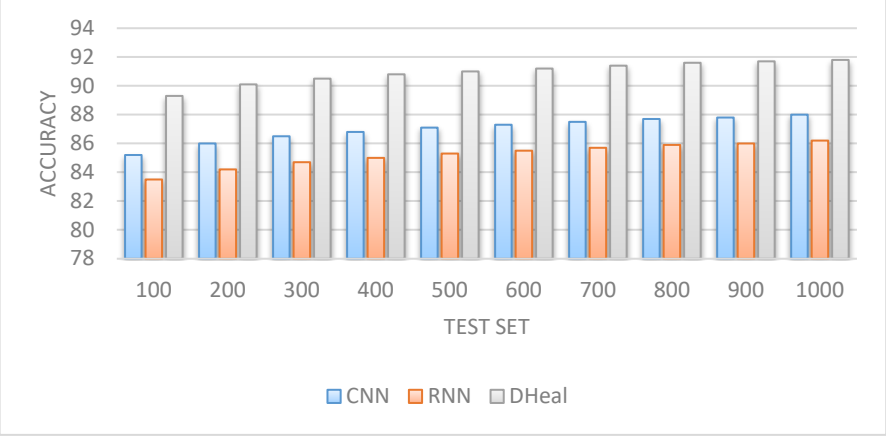

Figure 2. Accuracy (%)

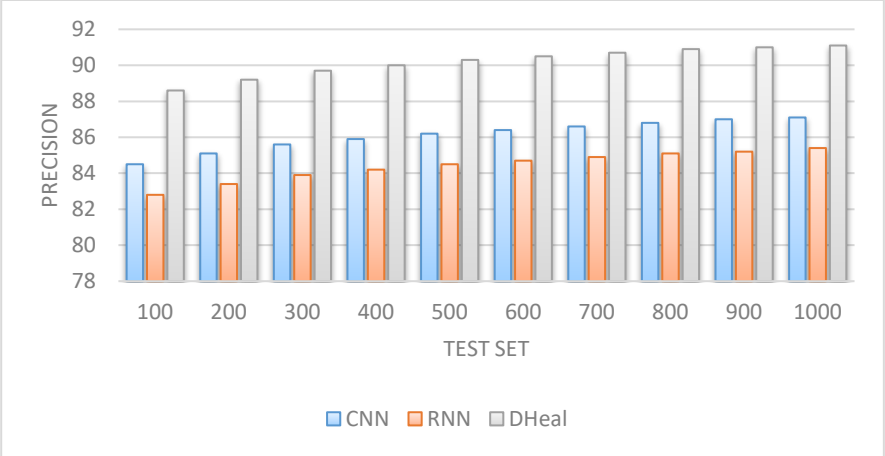

Figure 3. Precision (%)

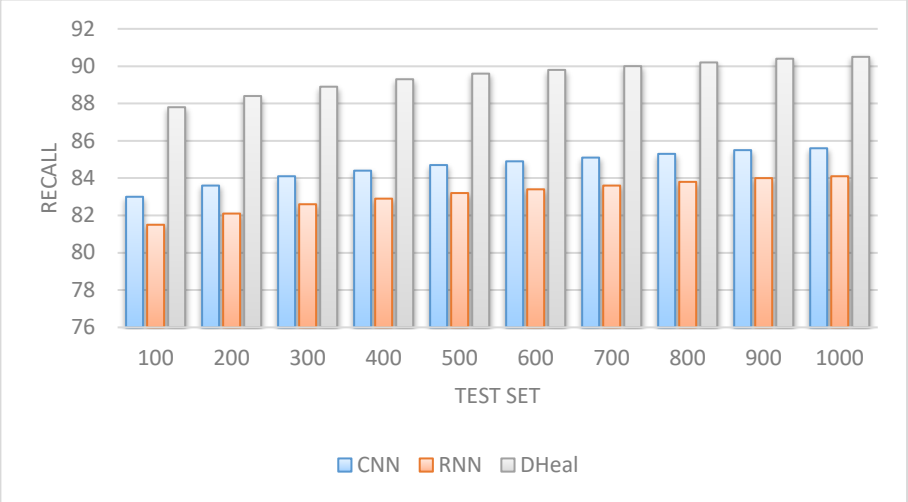

Figure 4. Recall (%)

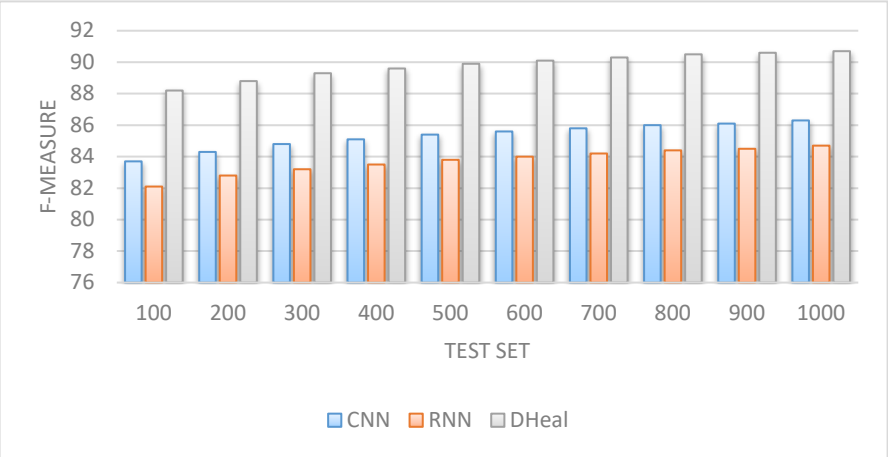

Figure 5. F-Measure (%)

Table 4. Loss (%)

Number of test datasets	CNN	RNN	DHeal
100	0.15	0.17	0.12
200	0.14	0.16	0.11
300	0.13	0.15	0.10
400	0.12	0.14	0.09
500	0.11	0.13	0.08
600	0.10	0.12	0.07
700	0.09	0.11	0.06
800	0.08	0.10	0.05
900	0.07	0.09	0.04
1000	0.06	0.08	0.03

Table 5. ROC

Number of test datasets	CNN	RNN	DHeal
100	0.87	0.85	0.91
200	0.88	0.86	0.92
300	0.89	0.87	0.93
400	0.89	0.88	0.93
500	0.90	0.88	0.94
600	0.90	0.89	0.94
700	0.91	0.89	0.95
800	0.91	0.90	0.95
900	0.91	0.90	0.95
1000	0.92	0.90	0.96

Competitive results were shown by the range of recalls of the proposed DAE model from 88% to 98%. With F-measure values between 88% and 98%, the proposed DAE model routinely outperforms the competitors. This proves the reliability of the proposed DAE model in identifying and categorizing network anomalies. It further demonstrates the healthy ratio between recall and precision.

The RNN and DAE models achieved accuracy ranges of 94% ± 1.2% to 94% ± 1.3% and precision levels of 84% to 94%, respectively. Still, it was shown that the DAE model worked the best for identifying and mitigating cybersecurity threats in healthcare systems. Evidence of this came from the consistent outperformance of these models' overall evaluation criteria.

Our results show that the DAE paradigm has great potential to enhance intrusion detection and healthcare network security. The capacity of the proposed DAE model to identify irregular patterns of network traffic is one significant step in lowering potential hazards and protecting vital healthcare data.

CONCLUSION

The cybersecurity-based intrusion detection research done by the healthcare company produces generally good findings, and the proposed DAE model performs amazingly well. Research on a dataset with a thousand examples revealed that the DAE model has impressive accuracy rates, up to 98%.

The practical implications of the findings are significant for healthcare institutions aiming to enhance their cybersecurity measures. DeepHeal, leveraging Deep Autoencoders (DAE), offers a flexible and effective solution for integrating anomaly detection into existing security infrastructures.

Future research should explore hybrid AI models that combine the strengths of multiple deep learning architectures, such as combining DAEs with recurrent neural networks (RNNs) for temporal anomaly detection.

REFERENCES

Ahuja, K., Bala, I., & Mijwil, M. M. (2024). Industry 4.0 in manufacturing, communication, transportation, and healthcare. In A. K. Rana, V. Sharma, A. Rana, M. Alam, & S. L. Tripathi (Eds.*), Convergence of blockchain and internet of things in healthcare* (pp. 25-53). CRC Press. https://doi.org/10.1201/9781003466949-2

Bortsova, G., González-Gonzalo, C., Wetstein, S. C., Dubost, F., Katramados, I., Hogeweg, L., Liefers, B., van Ginneken, B., Pluim, J. P. W., Veta, M., Sánchez, C. I., & de Bruijne, M. (2021). Adversarial attack vulnerability of medical image analysis systems: Unexplored factors. *Medical Image Analysis*, *73*, 102141. https://doi.org/10.1016/j.media.2021.102141

Costa, J. C., Roxo, T., Proença, H., & Inácio, P. R. (2024). How deep learning sees the world: A survey on adversarial attacks & defenses. *IEEE Access*, *12*, 61113-61136. https://doi.org/10.1109/ACCESS.2024.3395118

Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., Garcia, N. M., & Zdravevski, E. (2021). *IoT healthcare security dataset*. GibHug.

Kaviani, S., Han, K. J., & Sohn, I. (2022). Adversarial attacks and defenses on AI in medical imaging informatics: A survey. *Expert Systems with Applications*, *198*, 116815. https://doi.org/10.1016/j.eswa.2022.116815

Liu, N., Du, M., Guo, R., Liu, H., & Hu, X. (2021). Adversarial attacks and defenses: An interpretation perspective. *ACM SIGKDD Explorations Newsletter*, *23*(1), 86-99. https://doi.org/10.1145/3468507.3468519

Ma, X., Niu, Y., Gu, L., Wang, Y., Zhao, Y., Bailey, J., & Lu, F. (2021). Understanding adversarial attacks on deep learning based medical image analysis systems. *Pattern Recognition*, *110*, 107332. https://doi.org/10.1016/j.patcog.2020.107332

Maguluri, L. P., Santhosh, K.; Meenakshi, K., Farooqui, M. A., Sultana, H. P., & Saravanan, V. (2023, May). An artificial intelligence based machine learning approach for automatic blood glucose level identification of diabetes patients. *Proceedings of the International Conference on Disruptive Technologies, Greater Noida, India*, 104-109. https://doi.org/10.1109/ICDT57929.2023.10150866

Newaz, A. I., Haque, N. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2020, December). Adversarial attacks to machine learning-based smart healthcare systems. *Proceedings of the IEEE Global Communications Conference*, *Taipei, Taiwan*, 1-6. https://doi.org/10.1109/GLOBECOM42002.2020.9322472

Puttagunta, M. K., Ravi, S., & Nelson Kennedy Babu, C. (2023). Adversarial examples: Attacks and defenses on medical deep learning systems. *Multimedia Tools and Applications*, *82*(22), 33773-33809. https://doi.org/10.1007/s11042-023-14702-9

Rahman, A., Hossain, M. S., Alrajeh, N. A., & Alsolami, F. (2020). Adversarial examples – Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet of Things Journal*, *8*(12), 9603-9610. https://doi.org/10.1109/JIOT.2020.3013710

Saravanan, V., Parameshachari, B. D., Hussein, A. H. A., Shilpa, N., & Adnan, M. M. (2023, November). Deep learning techniques based secured biometric authentication and classification using ECG signal. *Proceedings of the International Conference on Integrated Intelligence and Communication Systems, Kalaburagi, India*, 1-5. https://doi.org/10.1109/ICIICS59993.2023.10421295

Saravanan, V., Sankaradass, V., Shanmathi, M., Bhimavarapu, J. P., Deivakani, M., & Ramasamy, S. (2023, May). An early detection of ovarian cancer and the accurate spreading range in human body by using deep medical learning model. *Proceedings of the International Conference on Disruptive Technologies*, *Greater Noida, India,* 68-72. https://doi.org/10.1109/ICDT57929.2023.10151103

Selvaganapathy, S. G., & Sadasivam, S. (2021). Healthcare security: Usage of generative models for malware adversarial attacks and defense. In H. Sharma, M. K. Gupta, G. S. Tomar, & W. Lipo (Eds.),.*Communication and intelligent systems* (pp. 885-897). Springer. https://doi.org/10.1007/978-981-16-1089-9_68

Veerappan, K. N. G., Natarajan, Y., Raja, A., Perumal, J., & Kumar, S. J. (2023). Categorical data clustering using meta heuristic link-based ensemble method: Data clustering using soft computing techniques. In A. Suresh Kumar, U. Kose, S. Sharma, & S. Jerald Nirmal Kumar (Eds.), *Dynamics of swarm intelligence health analysis for the next generation* (pp. 226-238). IGI Global. https://doi.org/10.4018/978-1-6684-6894-4.ch012

Yuvaraj, N., Praghash, K., Arshath Raja, R., Chidambaram, S., & Shreecharan, D. (2022). Hyperspectral image classification using denoised stacked auto encoder-based restricted Boltzmann machine classifier. In A. Abraham, T. P. Hong, K. Kotecha, K. Ma, P. Manghirmalani Mishra, & N. Gandhi (Eds.), *Hybrid intelligent systems* (pp. 213-221). Springer. https://doi.org/10.1007/978-3-031-27409-1_19

Zhang, C., Costa-Perez, X., & Patras, P. (2022). Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms. IEEE/ACM Transactions on Networking, *30*(3), 1294-1311. https://doi.org/10.1109/TNET.2021.3137084

AUTHOR

Dr A. Mekala is an Assistant Professor at the Sacred Heart College, Tirupattur. She has published research articles in national and international journals and presented papers at various national and international conferences. Her specialization field is ontology and text mining. She has published two books on computer networks, software testing, and quality assurance.

Mrs Shahnaz Fatima has an undergraduate and an MS by research from JNTUH and is currently pursuing a PhD at JNTUK. She has 16 years of experience as a faculty member in India and Ethiopia. Currently, she is an assistant professor in the ECE department at Sasi Institute of Technology and Engineering, Andhra Pradesh.

Dr. B. V. Subba Rao is a professor and IT head at P.V.P Siddhartha Institute of Technology Vijayawada, affiliated with Jawaharlal Nehru Technological University. He has 23 years of rich experience in teaching, research, and industry. He received his PhD and M.Tech degrees with distinction in Computer Science and Engineering from Acharya Nagarjuna University. His research interests are artificial intelligence, natural language processing, and information retrieval systems.

Dr. J Rajendra Prasad is a Professor at NRI Institute of Technology, Agiripalli, Vijayawada, affiliated with Jawaharlal Nehru Technological University. He has 36 years of experience in teaching. He received his PhD from Andhra University. He has guided 23 postgraduate and 35 graduate projects. He has published several papers. His research interests are in the areas of data science and data mining.

Mrs. P. G. Banupriya has 12 years of teaching experience. She is an Assistant Professor in the Department of Computer Science and Engineering, Karpagam Institute of Technology, Coimbatore. Her areas of interest are cloud computing, machine learning, and web applications. She is currently pursuing research in the area of network and information security.

Mr. K. Venkataramana was born in Srikalahasti, Andhra Pradesh, India, on March 28, 1985. Since 2008, he has been an Associate Professor in the Department of CSE, QIS College of Engineering and Technology, Ongole, India. His research interests are MANETs and cloud computing.