Anomaly Detection in IoT-Based Healthcare Networks Using Hybrid Deep Learning Models

[1]Dr.M.Thejovathi, [2]Padala S Venkata Durga Gayatri, [3]K.SaiKeerthi,
[4]M.S.D.K.Durga,[5]MD. Aazma, [6] M.Sowjanya
[1]Associate Professor, CSE(AI &ML)[(3,4,5,6)]
[3,4,5,6]B.Tech 3rd year Student, CSE(AI &ML),
Vignan's Institute ofManagement and Technology for Women, Hyderabad, India
[2]Associate Professor, Department of CSE, University College of Engineering, Adikavi Nannayya University, Rajamahendravaram, AP
[1] thejovathi@vmtw.in , [2]gayatri.cse@aknu.edu.in [3]kalakotakeerthy@gmail.com ,
[3]durga01.madala@gmail.com,[4] azma9812@gmail.com , [5] sowjanyamantri25@gmail.com,

Abstract

The abstract states that IoT in healthcare is rapidly advancing, enhancing patient care through remote monitoring and automated diagnosis. However, these systems face security threats such as brute force attacks, spoofing, DDoS attacks, and data manipulation, which can compromise patient data and system performance. To address these challenges, the project proposes a hybrid deep learning model that integrates CNN for feature extraction, LSTM for sequence pattern detection, and Autoencoders for recognizing abnormal behaviors. This model enhances detection accuracy, reduces false alerts, and ensures a faster response to threats. The model is tested on IoT healthcare datasets and effectively detects threats like malware injection, unauthorized access, and network intrusions, thereby improving security and ensuring reliable healthcare data protection.

Keywords: IoT Networks, Healthcare, Anomaly Detection, Deep Learning, CNN, LSTM, Cyber threats, Data manipulation.

I. Introduction

The Internet of Things (IoT) is changing healthcare by connecting medical devices, sensors, and monitoring systems together. This technology helps doctors and hospitals collect patient information in real-time, allowing for faster and better decision-making. Smart devices like wearable health trackers, remote patient monitors, and automated alert systems have made it easier to detect health problems early and provide personalized care. However, as more devices get connected, healthcare networks face serious risks. Cyberattacks like **data manipulation**, **device spoofing**, and **DDoS attacks** can harm patients by giving wrong medical readings, thus, strong security systems are needed to protect patient data and ensure that devices work reliably. In this project, we propose a **hybrid deep learning model** that improves the detection of security threats in healthcare IoT networks, making healthcare smarter, safer, and more reliable.

Role of IoT in Healthcare

IoT technology has made healthcare more effective by allowing continuous tracking of patients' health without needing them to be in the hospital. Wearable sensors can measure vital signs like heart rate, oxygen level, and blood pressure. Doctors can monitor patients from anywhere,Hospitals also benefit from IoT by creating **smart hospitals** where devices

manage equipment, track medicines, and optimize patient care. This reduces human errors, saves time, and ensures that healthcare services are more efficient and patient-friendly.

B. Importance of Anomaly Detection

In healthcare, even a small mistake can be dangerous. If a patient's vital signs suddenly change, or if a device is hacked or sends wrong data, it can put the patient's life at risk.

Anomaly detection is the process of finding unusual activities or patterns that do not match normal behavior. It helps in spotting early signs of cyberattacks, device failures, or patient emergencies. Real-time anomaly detection makes sure that problems are found immediately, so healthcare staff can act quickly to fix them. This improves patient safety, keeps healthcare services running smoothly, and protects sensitive medical information.

C. Challenges in IoT-Based Healthcare

While IoT brings many benefits, it also comes with big challenges:

- **Security Risks**: Many IoT devices have weak security and can be attacked easily.
- **Different Standards**: Devices from different companies may not work together properly, causing communication problems (interoperability issues).
- **Big Data Management**: Healthcare IoT produces a massive amount of data every day. Handling, storing, and analyzing this data quickly and securely is very difficult.
- **Resource Limitations**: Most IoT devices have low computing power and battery life, so heavy security solutions cannot be used on them. Because of these challenges, smarter, faster, and lightweight security systems are urgently needed.

D. Motivation

The main motivation behind this project is to make healthcare IoT systems safer and smarter. With the growing number of cyberattacks targeting healthcare, there is an urgent need for real-time, accurate, and lightweight anomaly detection systems. Our hybrid deep learning model, combining **CNN**, **LSTM**, and **Autoencoders**, is designed to meet these needs by detecting both known and unknown threats with high accuracy and fewer false alarms.

By doing this, we aim to protect patient lives, maintain trust in healthcare systems, and support the safe growth of IoT technology in the medical field.

II. Modules

A. Convolutional Neural Network (CNN)

Purpose in Hybrid Architecture:

Convolutional Neural Networks (CNNs) are primarily used to capture spatial relationships in data. In the context of network traffic analysis, spatial features may refer to relationships between various packet attributes such as source IP, destination IP, protocol

type, and port numbers. CNNs, originally designed for image recognition, are highly effective in extracting local features due to their convolutional and pooling operations.

The proposed model uses a 1D CNN layer to process sequential network flow features. This configuration involves:

- Convolutional filters that slide over the input vectors representing traffic flows.
- ReLU (Rectified Linear Unit) activation functions to introduce non-linearity.
- MaxPooling to reduce the spatial dimension and focus on dominant features.

Mathematically, the output of a 1D convolution operation for a given filter
ff and input sequence

$$y_i = \text{ReLU}\left(\sum_{j=0}^{k-1} f_j \cdot x_{i+j} + b\right)$$

where ,
k is the kernel size, and
b is the bias term.

This representation ensures that the model captures significant spatial relationships within the network packets, which are then passed to the LSTM for temporal processing

B.Long Short-Term Memory (LSTM)

Purpose in Hybrid Architecture:

LSTM networks are specialized Recurrent Neural Networks (RNNs) designed to handle long-range dependencies in sequential data. Network traffic inherently contains temporal dependencies—certain attacks like DDoS or brute force attacks unfold over time and are better captured using sequential models.

Architectural Description:

The LSTM block in the proposed model processes the output from the CNN or directly ingests sequential traffic feature vectors. It consists of memory cells, input gates, output gates, and forget gates, which collectively manage the flow of information across time steps.

Each LSTM unit follows the equations:

$$\begin{aligned}
f_t &= \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \\
i_t &= \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \\
\tilde{C}_t &= \tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \\
C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t \\
o_t &= \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \\
h_t &= o_t * \tanh(C_t)
\end{aligned}$$

This gating mechanism allows the LSTM to preserve relevant features and discard irrelevant information, making it suitable for capturing evolving attack patterns over time.

C. Autoencoder

Purpose in Hybrid Architecture:

Autoencoders are unsupervised neural networks used for feature learning and anomaly detection. They are particularly effective in modeling the normal behavior of network traffic. Any significant deviation from this normal behavior, measured by reconstruction loss, is flagged as an anomaly.

Architectural Description:

An autoencoder consists of two symmetric parts:

Encoder: Compresses the input into a lower-dimensional latent space.

Decoder: Attempts to reconstruct the input from the encoded representation.

Formally, if x is the input and $\hat{x}$ is the reconstruction:

$$\hat{x} = D(E(x))$$

where E and D are the encoder and decoder functions respectively.

The **reconstruction error** is computed using Mean Squared Error (MSE):

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2$$

This error serves as an anomaly score. Higher values indicate anomalous patterns not seen during training.

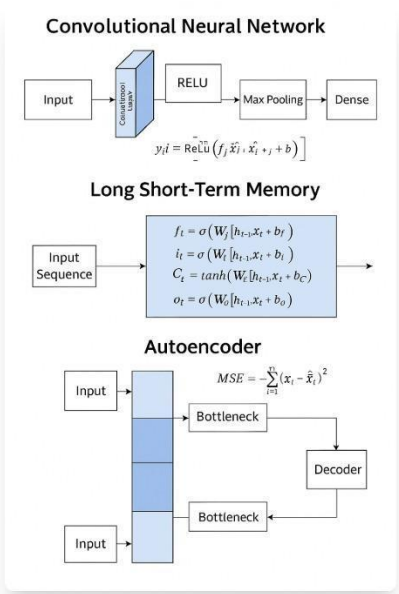
Fusion and Classification Layer

The outputs from the CNN-LSTM stream and the Autoencoder branch are concatenated to form a comprehensive feature vector. This vector is passed through:

One or more fully connected layers to learn complex interactions,

A final Soft max layer that performs classification between normal and anomalous traffic instances.

This ensemble structure enhances the model's ability to detect known and unknown threats by combining spatial, temporal, and statistical perspectives.



III. Literature Survey

This paper used HMM and SVM for real-time anomaly detection in healthcare IoT and achieved 98.66% accuracy. The method works well but depends on fixed data parts and manual features, which makes it less flexible [1]. This study reviewed 44 research works and found that deep learning methods like CNN and LSTM help in disease prediction and health monitoring. However, most models need large datasets, high computing power, and are hard to understand [2]. This paper introduced a fog computing and blockchain-based system with a swarm optimization algorithm. It achieved 99.7% accuracy with low energy use but may not work well with many IoT devices due to its complexity [3]. This work applied machine learning models (like Random Forest and DNN) on the CIC IoT dataset. It gave 99.55% accuracy but had issues with detecting spoofing attacks and needed more real-world testing [4]. This paper used a hybrid deep learning model with SVM for smart hospital IoT. It reduced false alarms and worked fast, but had problems with high false positives and did not perform well on large IoT networks [5].

IV. Future Scope

Looking ahead, there is significant potential to advance the field of IoT security in healthcare. Developing high-quality, annotated datasets specifically for healthcare IoT scenarios would significantly enhance the training and evaluation of threat detection models. Future systems must focus on achieving real-time, low-latency processing to ensure timely responses without overwhelming computational resources. There is a growing need for adaptive and generalizable security models capable of detecting new and unknown threats with minimal human intervention. Addressing the issues of false positives and false negatives through more accurate detection algorithms will also be critical for building trust in these systems. Furthermore, enhancing the explainability and interpretability of threat detection

models will be essential for gaining acceptance among healthcare practitioners, who require understandable and actionable insights. By addressing these research gaps, future solutions can create more resilient, efficient, and reliable healthcare IoT environments.

V. Algorithm:

1. Collect Dataset

- Use an IoT healthcare dataset (e.g., CICIoT, CICIDS2017).
- Ensure the dataset has both normal and attack data.

2. Preprocess Data

- Clean the data (remove missing values).
- Normalize the values.
- Extract useful features.

3. Build CNN Model

- Apply Convolutional Neural Networks to extract spatial features from the data.

4. Add LSTM Layer

- Use Long Short-Term Memory (LSTM) to learn time-based patterns.

5. Use Autoencoder

- Apply an Autoencoder to detect anomalies by comparing input and reconstructed output.

6. Train the Model

- Use the preprocessed data to train the hybrid CNN-LSTM-Autoencoder model.

7. Evaluate the Model

- Check model performance using Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.

8. Detect Anomalies

- Use the trained model to detect attacks like spoofing, DDoS, and unauthorized access in real time

VI.Result:

Precision, recall , f1-score

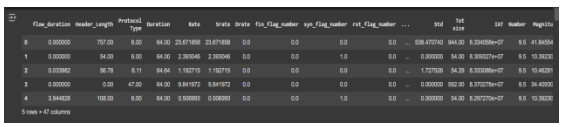
```
from sklearn.metrics import classification_report

print("Classification Report:")
print(classification_report(y_test, y_pred))
```

```
Classification Report:
              precision    recall  f1-score   support

           0       0.00      0.00      0.00        10
           1       0.73      0.97      0.83      2263
           2       0.00      0.00      0.00         7
           3       1.00      0.08      0.15        12
           4       1.00      0.99      0.99       570
           5       0.51      0.67      0.58        55
           6       1.00      1.00      1.00     14837
           7       0.99      0.98      0.98       971
           8       1.00      1.00      1.00      8325
           9       1.00      1.00      1.00      8184
          10       0.67      0.97      0.79      8407
          11       0.54      0.61      0.57        49
          12       0.97      0.58      0.73      7410
          13       0.64      0.96      0.77      9184
          14       0.77      0.91      0.83     11076
          15       0.99      0.98      0.99       548
          16       0.55      0.25      0.34       376
          17       1.00      0.25      0.40        24
          18       0.80      0.71      0.75       136
          19       0.61      0.49      0.54      4187
          20       0.60      0.10      0.17      5514
          21       0.80      0.55      0.65      6790
          22       0.81      0.55      0.66       622
          23       0.97      0.92      0.94      2033
          24       0.90      0.95      0.93      1556
          25       0.99      1.00      0.99      1909
          26       0.68      0.59      0.63       257
          27       0.32      0.12      0.17       198
          28       0.00      0.00      0.00         6
          29       0.46      0.19      0.27       173
```

```
          12       0.97      0.58      0.73      7410
          13       0.64      0.96      0.77      9184
          14       0.77      0.91      0.83     11076
          15       0.99      0.98      0.99       548
          16       0.55      0.25      0.34       376
          17       1.00      0.25      0.40        24
          18       0.80      0.71      0.75       136
          19       0.61      0.49      0.54      4187
          20       0.60      0.10      0.17      5514
          21       0.80      0.55      0.65      6790
          22       0.81      0.55      0.66       622
          23       0.97      0.92      0.94      2033
          24       0.90      0.95      0.93      1556
          25       0.99      1.00      0.99      1909
          26       0.68      0.59      0.63       257
          27       0.32      0.12      0.17       198
          28       0.00      0.00      0.00         6
          29       0.46      0.19      0.27       173
```

```
          30       0.00      0.00      0.00        11
          31       0.00      0.00      0.00         3
          32       0.55      0.87      0.68        83
          33       0.00      0.00      0.00         7
          34       0.00      0.00      0.00         1

    accuracy                           0.83     95794
   macro avg       0.62      0.55      0.55     95794
weighted avg       0.84      0.83      0.81     95794
```

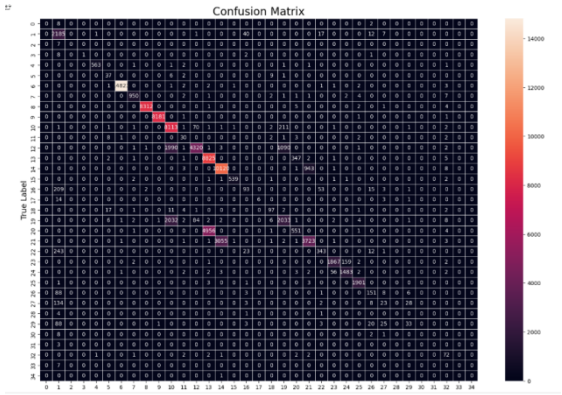
Sample Dataset:



Accuracy:

```
2994/2994 ━━━━━━━━━━━━━━━━━━━━ 30s 10ms/step - accuracy: 0.8278 - loss: 0.3856
Test Accuracy: 0.8286
```

Confusion Matrix:



VII. Conclusion

The security of healthcare IoT systems is of critical importance as these technologies become more deeply embedded in patient care and medical operations. Current threat detection mechanisms face several limitations, including high false alarm rates, poor adaptability to emerging threats, inefficiencies in large-scale deployments, and high computational demands that limit their use in low-power devices. These challenges highlight the urgent need for more advanced, efficient, and reliable security solutions. Addressing real-time processing demands, improving model adaptability, and ensuring better accuracy in threat detection will play a crucial role in strengthening healthcare IoT systems. Furthermore, building models that are interpretable and explainable will be vital for their adoption in clinical environments. Overall, with focused research and technological innovation, it is possible to create healthcare IoT ecosystems that are not only smart and efficient but also resilient against evolving cyber security threats.

References

1. https://www.unb.ca/cic/datasets/ids-2017.html
2. UNSW-NB15 Dataset. Australian Centre for Cyber Security. https://research.unsw.edu.au/projects/unsw-nb15-dataset
3. S. H. Hashemi, S. M. Ghasemi, and S. Samet, “Intrusion detection in IoT-based systems using machine learning algorithms: A survey,” *Journal of Network and Computer Applications*, vol. 192, 2021, doi: 10.1016/j.jnca.2021.103164.
4. D. Singh, V. Sharma, and A. Ghosh, “Anomaly detection for IoT-based healthcare systems using machine learning techniques,” *Procedia Computer Science*, vol. 132, pp. 1043–1050, 2018.
5. D Shanthi, Smart Healthcare for Pregnant Women in Rural Areas, Medical Imaging and Health Informatics, Wiley Publishers,ch-17, pg.no:317-334, 2022, https://doi.org/10.1002/9781119819165.ch17
6. Shanthi, R. K. Mohanty and G. Narsimha, "Application of machine learning reliability data sets", Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS), pp. 1472-1474, 2018.
7. D Shanthi, N Swapna, Ajmeera Kiran and A Anoosha, "Ensemble Approach Of GPACOTPSOAnd SNN For Predicting Software Reliability", International Journal Of Engineering Systems Modelling And Simulation, 2022.
8. Shanthi, "Ensemble Approach of ACOT and PSO for Predicting Software Reliability", 2021 Sixth International Conference on Image Information Processing (ICIIP), pp. 202-207, 2021.

9. D Shanthi, CH Sankeerthana and R Usha Rani, "Spiking Neural Networks for Predicting Software Reliability", ICICNIS 2020, January 2021, [online] Available: https://ssrn.com/abstract=3769088.
10. Shanthi, D. (2023). Smart Water Bottle with Smart Technology. In Handbook of Artificial Intelligence (pp. 204-219). Bentham Science Publishers.
11. Shanthi, P. Kuncha, M. S. M. Dhar, A. Jamshed, H. Pallathadka and A. L. K. J E, "The Blue Brain Technology using Machine Learning," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1370-1375, doi: 10.1109/ICCES51350.2021.9489075.
12. Shanthi, D., Aryan, S. R., Harshitha, K., & Malgireddy, S. (2023, December). Smart Helmet. In International Conference on Advances in Computational Intelligence (pp. 1-17). Cham: Springer Nature Switzerland.
13. Babu, Mr. Suryavamshi Sandeep, S.V. Suryanarayana, M. Sruthi, P. Bhagya Lakshmi, T. Sravanthi, and M. Spandana. 2025. "Enhancing Sentiment Analysis With Emotion And Sarcasm Detection: A Transformer-Based Approach". Metallurgical and Materials Engineering, May, 794-803. https://metall-mater-eng.com/index.php/home/article/view/1634.
14. Narmada, J., Dr.A.C.Priya Ranjani, K. Sruthi, P. Harshitha, D. Suchitha, and D.Veera Reddy. 2025. "Ai-Powered Chacha Chaudhary Mascot For Ganga Conservation Awareness". Metallurgical and Materials Engineering, May, 761-66. https://metall-mater-eng.com/index.php/home/article/view/1631.
15. Geetha, Mrs. D., Mrs.G. Haritha, B. Pavani, Ch. Srivalli, P. Chervitha, and Syed. Ishrath. 2025. "Eco Earn: E-Waste Facility Locator". Metallurgical and Materials Engineering, May, 767-73. https://metall-mater-eng.com/index.php/home/article/view/1632.
16. P. Shilpasri PS, C.Mounika C, Akella P, N.Shreya N, Nandini M, Yadav PK. Rescuenet: An Integrated Emergency Coordination And Alert System. J Neonatal Surg [Internet]. 2025May13 [cited 2025May17];14(23S):286-91. Available from: https://www.jneonatalsurg.com/index.php/jns/article/view/5738
17. D. Shanthi DS, G. Ashok GA, Vennela B, Reddy KH, P. Deekshitha PD, Nandini UBSB. Web-Based Video Analysis and Visualization of Magnetic Resonance Imaging Reports for Enhanced Patient Understanding. J Neonatal Surg [Internet]. 2025May13 [cited 2025May17];14(23S):280-5. Available from: https://www.jneonatalsurg.com/index.php/jns/article/view/5733
18. Srilatha, Mrs. A., R. Usha Rani, Reethu Yadav, Ruchitha Reddy, Laxmi Sathwika, and N. Bhargav Krishna. 2025. "Learn Rights: A Gamified Ai-Powered Platform For Legal Literacy And Children's Rights Awareness In India". Metallurgical and Materials Engineering, May, 592-98. https://metall-mater-eng.com/index.php/home/article/view/1611.
19. Shanthi, Dr. D., G. Ashok, Chitrika Biswal, Sangem Udharika, Sri Varshini, and Gopireddi Sindhu. 2025. "Ai-Driven Adaptive It Training: A Personalized Learning Framework For Enhanced Knowledge Retention And Engagement". Metallurgical and Materials Engineering, May, 136-45. https://metall-mater-eng.com/index.php/home/article/view/1567.
20. P. K. Bolisetty and Midhunchakkaravarthy, "Comparative Analysis of Software Reliability Prediction and Optimization using Machine Learning Algorithms," 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 2025, pp. 1-4, doi: 10.1109/ICISCN64258.2025.10934209.
21. Priyanka, Mrs. T. Sai, Kotari Sridevi, A. Sruthi, S. Laxmi Prasanna, B. Sahithi, and P. Jyothsna. 2025. "Domain Detector - An Efficient Approach of Machine Learning for Detecting Malicious Websites". Metallurgical and Materials Engineering, May, 903-11.
22. Thejovathi, Dr. M., K. Jayasri, K. Munni, B. Pooja, B. Madhuri, and S. Meghana Priya. 2025. "Skinguard-Ai FOR Preliminary Diagnosis OF Dermatological Manifestations". Metallurgical and Materials Engineering, May, 912-16.
23. Jayanna, SP., S. Venkateswarlu, B. Ishwarya Bharathi, CH. Mahitha, P. Praharshitha, and K. Nikhitha. 2025. "Fake Social Media Profile Detection and Reporting". Metallurgical and Materials Engineering, May, 965-71.
24. D Shanthi, "Early-stage breast cancer detection using ensemble approach of random forest classifier algorithm", Onkologia i Radioterapia 16 (4:1-6), 1-6, 2022.
25. D Shanthi, "The Effects of a Spiking Neural Network on Indian Classical Music", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.9, Issue 3, page no. ppa195-a201, March-2022

26. Parupati K, Reddy Kaithi R. Speech-Driven Academic Records Delivery System. J Neonatal Surg [Internet]. 2025Apr.28 [cited 2025May23];14(19S):292-9. Available from: https://www.jneonatalsurg.com/index.php/jns/article/view/4767
27. Dr.D.Shanthi and Dr.R.Usha Rani, " Network Security Project Management", ADALYA JOURNAL, ISSN NO: 1301-2746, PageNo: 1137 – 1148, Volume 9, Issue 3, March 2020 DOI:16.10089.AJ.2020.V9I3.285311.7101
28. D. Shanthi, R. K. Mohanthy, and G. Narsimha, "Hybridization of ACOT and PSO to predict Software Reliability ", *International Journal Pure and Applied Mathematics*, Vol. 119, No. 12, pp. 13089 - 13104, 2018.
29. D. Shanthi, R.K. Mohanthy, and G. Narsimha, "Application of swarm Intelligence to predict Software Reliability ", *International Journal Pure and Applied Mathematics*, Vol. 119, No. 14, pp. 109 - 115, 2018.
30. Srilatha, Mrs. A., R. Usha Rani, Reethu Yadav, Ruchitha Reddy, Laxmi Sathwika, and N. Bhargav Krishna. 2025. "Learn Rights: A Gamified Ai-Powered Platform For Legal Literacy And Children's Rights Awareness In India". Metallurgical and Materials Engineering, May, 592-98.