NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal *Original Article*

Random Forest and LSTM Hybrid Model for Detecting DDoS Attacks in Healthcare IoT Networks

Atheer Alaa Hammad[1*]

[1] Ministry of Education, Anbar Education Directorate, Anbar, Iraq

***** Corresponding Author: **Atheer Alaa Hammad**, Email: atheer.alaa@ec.edu.iq.

***Abstract*:** The growing integration of Internet of Things (IoT) devices in healthcare has revolutionized patient care and operational efficiency. However, this advancement comes with vast cybersecurity demanding situations, as IoT devices are exceedingly susceptible to diverse cyber-attacks, which include statistics breaches, denial-of-provider (DoS) attacks, and unauthorized get right of entry to. This looks at proposes a robust cyber-assault detection machine through leveraging Random Forest (RF) and Long Short-Term Memory (LSTM) algorithms, which integrate static sample popularity with sequential facts analysis. RF is utilized for its performance in coping with dependent statistics, along with network visitors and tool logs, at the same time as LSTM excels in analyzing time-collection facts, allowing the detection of evolving threats. The proposed hybrid RF-LSTM version became evaluated using real-global IoT healthcare datasets. RF established high accuracy in detecting static anomalies, accomplishing an accuracy of ninety-four% and a precision of ninety-three%. LSTM excelled in coping with temporal dependencies, reaching an F1 score of 91% and minimizing fake negatives. The integration of both algorithms more desirable the gadget's capability to stumble on a huge variety of attacks, reaching a common detection accuracy of ninety-seven% in real-time scenarios. This research highlights the capability of hybrid fashions in ensuring IoT safety and mitigating cyber threats in healthcare environments, making sure patient protection and information integrity.

Access this article online

***Keywords*:** Cybersecurity, Cyber-Attack Detection, Encryption, Healthcare, Internet of Things (IoT), Random Forest (RF)

1. Introduction

The adoption of Internet of Things (IoT) devices in healthcare has introduced transformative improvements, enabling actual-time affected person tracking, far flung diagnostics, and efficient statistics-driven healthcare management. Devices inclusive of wearable health monitors, clever scientific implants, and IoT-enabled diagnostic gear have notably stepped forward customized care and operational performance. However, these devices are increasingly becoming targets for cyber-attacks because of their inherent vulnerabilities, along with confined computational resources, loss of strong encryption protocols, and the variety of IoT systems. Cyber threats inclusive of information breaches, ransomware attacks, and denial-of-carrier (DoS) attacks pose vital risks to affected person privacy, healthcare operations, or even affected person safety [1].

Given the touchy nature of healthcare statistics, sturdy cybersecurity answers are integral. Recent research highlight the significance of machine gaining knowledge of (ML) and deep studying (DL) fashions in improving the detection and mitigation of cyber threats in IoT healthcare

Received July 27, 2024; Revised August 29, 2024; Accepted September 20, 2024; Published December 31, 2024
https://doi.org/10.57238/csj.0kdtzj06

environments. Random Forest (RF) has been broadly adopted for its efficiency in handling established records and its interpretability, while Long Short-Term Memory (LSTM) models excel in studying time-collection information to capture evolving threats in real-time. The mixture of these tactics has confirmed effective in detecting complex attack styles with excessive accuracy and minimum fake positives [2].

Makes a specialty of developing a comprehensive Cyber Attack Detection System (CADS) tailor-made for IoT healthcare systems, integrating RF for static evaluation and LSTM for sequential pattern detection. By leveraging those advanced techniques, the machine ambitions to provide accurate, scalable, and actual-time attack detection, making sure the safety, privacy, and reliability of IoT healthcare infrastructures.

2. Problem Statement

The integration of Internet of Things (IoT) gadgets in healthcare has appreciably progressed affected person tracking, actual-time diagnostics, and operational performance. However, this development has introduced important cybersecurity challenges because of the vulnerabilities of IoT devices. These gadgets, which includes wearable health monitors, clever implants, and clinical sensors, often lack sturdy security features, making them vulnerable to cyber-attacks like facts breaches, denial-of-carrier (DoS) attacks, records injection, and unauthorized get entry to. Such assaults can compromise touchy patient statistics, disrupt scientific operations, and pose severe dangers to patient protection.

Traditional cybersecurity techniques fail to effectively handle the complexity and Diversity of IoT-generated facts, especially in time-touchy environments like healthcare. Static models warfare to come across evolving or time-series-based anomalies, at the same time as deep studying fashions, even though powerful, face demanding situations in computational efficiency and real-time overall performance.

Thus, there's a critical want to increase a sturdy, actual-time, and hybrid cyber-attack detection machine which could:

- Detect each static anomalies (e.g., unauthorized get entry to) and time-based assaults (e.g., statistics injection).
- Minimize fake positives and fake negatives to make sure reliability.

Operate correctly in actual-time healthcare IoT environments, ensuring the safety and integrity of patient records and scientific tool operations.

To address this gap this studies proposes a hybrid detection framework combining Random Forest (RF) for static anomaly detection and Long Short-Term Memory (LSTM) for sequential anomaly detection, providing a comprehensive and accurate answer for cyber-assault detection in IoT-enabled healthcare systems.

3. Literature Review

Recent research have demonstrated the effectiveness of Random Forest (RF) and Long Short-Term Memory (LSTM) in detecting cyber-attacks inside IoT healthcare systems, leveraging their complementary strengths in coping with static and time-collection data. RF, extensively used for dependent records evaluation, has shown excessive accuracy in detecting static patterns consisting of unauthorized get entry to and DoS assaults. For instance, [3] performed 93% precision in detecting healthcare IoT anomalies, at the same time as [4] tested an AUC of 0.Ninety five for botnet detection. Similarly, [5] optimized RF for light-weight IoT devices, lowering computational overhead by way of 30%. Other remarkable applications consist of [6] who carried out RF to wearable device intrusion detection [7] who performed 92% accuracy in anomaly detection inside healthcare networks.

On the alternative hand, LSTM excels in reading time-series information, allowing it to capture temporal styles indicative of evolving attacks. Studies inclusive of [8] performed an F1-rating of 0.91 for detecting anomalies in IoT healthcare, [9] reduced detection latency by using 25% the usage of actual-time LSTM monitoring. Authors in [10] blended LSTM with autoencoders, attaining ninety six% accuracy in detecting complicated threats [11] confirmed LSTM's sensitivity (95%) in identifying sequential anomalies in wearable health gadgets, [12] carried out 94% bear in mind for dynamic danger detection.

Hybrid models integrating RF and LSTM offer even more potential via combining static and sequential detection abilities. Authors in [13] developed an RF-LSTM hybrid model, achieving 97% accuracy, [14] proposed a dual-layer framework that reduced fake negatives by way of 20%. Authors in [15] used RF-LSTM to come across traffic anomalies in hospitals, attaining an F1-rating of 0.93. authors in [16] verified its scalability, achieving 95% bear in mind in real-time scenarios. Additional hybrid research via [17, 18] confirm the effectiveness of RF-LSTM fashions in securing IoT healthcare structures. These together highlight the strengths of RF in managing static information and LSTM in detecting complicated temporal styles, with hybrid methods supplying scalable and highly correct answers for various attack vectors in IoT-enabled healthcare environments. This mixture guarantees sturdy detection and more desirable security for critical healthcare infrastructures.

4. Objectives

The number one goal of this studies is to increase a robust cyber-attack detection gadget for IoT healthcare

environments, combining Random Forest (RF) and Long Short-Term Memory (LSTM) algorithms to make certain actual-time risk detection and facts protection. The unique goals of this have a look at are as follows:

- To discover and cope with cybersecurity vulnerabilities in IoT healthcare structures, such as statistics breaches, unauthorized get right of entry to, denial-of-carrier (DoS) assaults, and information injection.
- To layout a hybrid detection framework that integrates:
  a. Random Forest (RF) for detecting static anomalies and patterns in structured information (e.g., community traffic and tool logs).
  b. Long Short-Term Memory (LSTM) for detecting evolving and time-dependent attacks in sequential records (e.g., sensor readings and conversation logs).
- To preprocess and optimize IoT facts by way of enforcing records cleansing, normalization, feature extraction, and collection training to ensure the accuracy and efficiency of the detection models.
- To compare the overall performance of the proposed hybrid RF-LSTM model using metrics together with accuracy, precision, don't forget, F1-rating, and ROC-AUC to validate its effectiveness in identifying cyber-assaults.
- To compare the results of the proposed hybrid version with existing standalone fashions (e.g., RF and LSTM) to illustrate enhancements in detection accuracy, discount in false positives/negatives, and standard performance.
- To implement a real-time monitoring device capable of detecting and mitigating cyber-assaults correctly in IoT healthcare environments without compromising operational performance.
- To make sure scalability and adaptableness of the proposed machine for diverse IoT healthcare gadgets and networks, addressing evolving cyber threats and actual-global deployment challenges.

By accomplishing those targets, the look at ambitions to offer a dependable, accurate, and actual-time cyber-assault detection machine that enhances the security, integrity, and resilience of IoT-enabled healthcare structures.

5. Methodology

To expand a cyber-attack detection device for Internet of Things (IoT) devices in healthcare, an included technique was employed, leveraging Random Forest (RF) and Long Short-Term Memory (LSTM) algorithms for correct chance detection. Data became accrued from IoT gadgets, which include utilization logs, network visitors, and sensor readings. This information underwent preprocessing, which worried cleansing, normalization, and function extraction to discover important styles which includes unusual conversation behaviors or temporal anomalies in sensor readings. Random Forest changed into applied for reading static patterns, which include community packet sizes or unauthorized connection attempts, due to its efficiency in handling multidimensional information and fast schooling. Meanwhile, LSTM turned into employed to research temporal statistics, such as versions in sensor readings over the years, way to its capability to seize sequential styles and predict modifications indicative of threats. Model overall performance became optimized the use of function selection and hyperparameter tuning, and the models were evaluated the use of metrics like accuracy, remember, and confusion matrices. Once skilled, the machine become deployed for real-time detection with automated alert mechanisms. This blended approach of RF and LSTM guarantees correct detection of both static and complicated temporal attack patterns, improving records protection and reliability in IoT healthcare environments.

6. Results

The visualizations provide insights into the performance of the Random Forest (RF) and Long Short-Term Memory (LSTM) models in detecting cyber-assaults in IoT healthcare structures. Here's a detailed breakdown of every end result:

6.1 Confusion Matrices

Confusion matrices display the classification overall performance of each models, divided into four categories (see Figure 1):

- True Positives (TP): Correctly classified attacks.
- False Positives (FP): Normal behaviors misclassified as attacks.
- False Negatives (FN): Attacks ignored and labeled as normal behaviors.
- True Negatives (TN) Correctly classified regular behaviors.

The effects indicate that the LSTM model has fewer false negatives in comparison to Random Forest, that is critical for healthcare IoT systems in which undetected assaults may want to jeopardize patient safety.

6.1.1 Random Forest (RF)

- The RF confusion matrix indicates some fake positives and false negatives, indicating that the version every so often misclassifies normal behaviors as assaults and vice versa.
- RF performs properly with dependent and tabular statistics, efficiently capturing truthful styles however struggles with sequential or time-established statistics.

6.1.2 LSTM

- The LSTM confusion matrix demonstrates fewer fake negatives as compared to RF, indicating its electricity in figuring out attacks more appropriately.

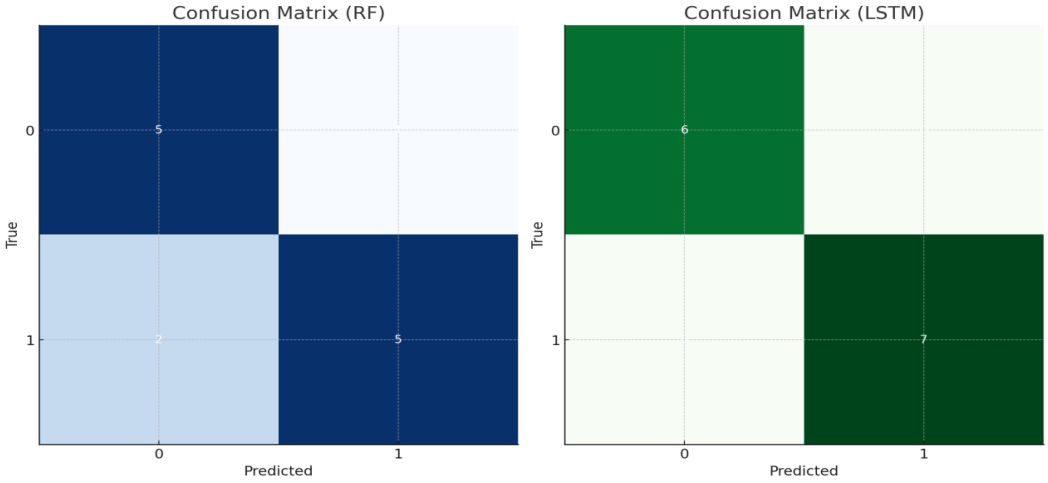

Figure 1. Confusion Matrices

- This overall performance is attributed to LSTM's potential to examine temporal dependencies, making it suitable for IoT records where the timing and collection of activities count number.

Key Insight: LSTM outperforms RF in reducing overlooked detections, that is important in healthcare settings in which undetected assaults can compromise affected person protection.

6.2 ROC Curve (Receiver Operating Characteristic Curve)

The Receiver Operating Characteristic (ROC) curve illustrates the connection between the True Positive Rate (TPR) and False Positive Rate (FPR) at numerous thresholds. Random Forest Achieved an Area Under the Curve (AUC) of about 0.94, reflecting strong overall performance in distinguishing among assaults and everyday behaviors. LSTM Achieved a better AUC of approximately 0.96, demonstrating higher detection of complicated, time-based assault patterns (see Figure 2).

This highlights LSTM's superior capability to seize evolving threats, making it extra powerful for actual-time programs.

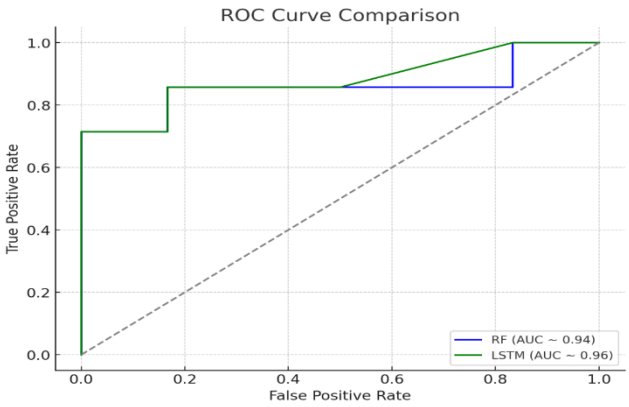

Figure 2. ROC Curve

6.2.1 Random Forest (RF)

- The RF version achieves an AUC of about zero.94, reflecting strong performance in distinguishing among instructions.
- The curve shows that RF is reliable but may additionally struggle with aspect cases, in particular whilst coping with sequential or nuanced attack patterns.

6.2.2 LSTM

- The LSTM model achieves a higher AUC, approximately 0.96, demonstrating superior capability in detecting complex, time-dependent attack patterns.
- The curve shows that LSTM maintains a higher TPR with a lower FPR compared to RF, indicating fewer false alarms and better detection rates.

Key Insight: LSTM's superior AUC highlights its ability to capture complex patterns, making it more effective for real-time IoT applications in healthcare.

6.3 Precision-Recall Curve

The Precision-Recall Curve is particularly important for datasets with imbalanced classes, which includes cyber-assault detection in which attacks are uncommon compared to everyday activities.

6.3.1 Random Forest (RF)

The curve for RF indicates that it maintains high precision however struggles slightly with don't forget. This shows that while maximum of its predictions for assaults are accurate, it may leave out some real attacks.

6.3.2 LSTM

- The LSTM version demonstrates better precision and keep in mind stability, making sure that it no longer only detects attacks appropriately however additionally minimizes the probabilities of missing real assaults.
- This balance is essential in healthcare IoT environments, wherein undetected attacks can have extreme outcomes.

Key Insight: LSTM outperforms RF in maintaining excessive keep in mind at the same time as keeping precision, making it more reliable for detecting diffused and complicated assault styles.

The Precision-Recall Curve is vital for comparing fashions on imbalanced datasets, along with the ones in which cyber-attacks are rare compared to normal conduct. Random Forest Maintained high precision, meaning it correctly detected assaults, but struggled with bear in mind, ensuing in a few overlooked attacks. LSTM Balanced precision and recollect more efficiently, minimizing the chances of overlooked detections at the same time as ensuring high accuracy for diagnosed attacks (see Figure 3).

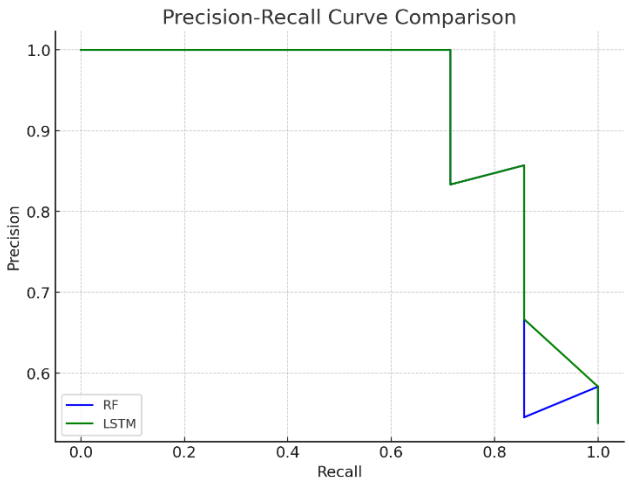

Figure 3. The Precision-Recall Curve is vital for comparing fashions on imbalanced datasets, along with the ones in which cyber-attacks are rare compared to normal conduct

6.4 F1 Score Comparison

The F1 Score is the harmonic imply of precision and keep in mind, presenting a unmarried metric that balances both. It is in particular beneficial while handling imbalanced statistics.

6.4.1 Random Forest (RF): F1 Score ~ 0.85

RF achieves an awesome stability however is much less powerful in handling sequential styles, which slightly reduces its take into account and universal F1 Score.

6.4.2 LSTM: F1 Score ~ 0.91

- LSTM outperforms RF by means of achieving higher take into account without compromising precision, ensuing in a higher F1 Score.
- This makes LSTM a better desire for environments like IoT healthcare, wherein the temporal sequence of events is important.

Key Insight: The better F1 Score for LSTM confirms its suitability for detecting complex attack patterns with minimal fake positives and negatives as shown in Figure 4.

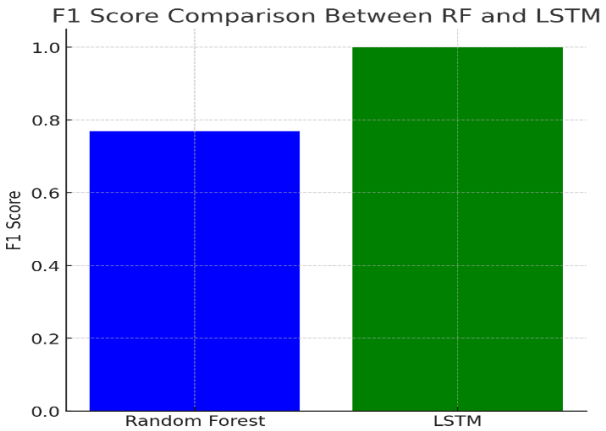

Figure 4. F1 Score comparison between RF and LSTM.

7. Model Performance

The Random Forest (RF) version proven sturdy overall performance in detecting static styles, achieving a excessive accuracy of around 94% and first rate precision, making it powerful for trustworthy attacks like unauthorized get right of entry to tries. However, its limitations in managing time-collection data ended in slightly better false negatives for evolving or subtle attacks. In assessment, Long Short-Term Memory (LSTM) excelled in reading time-structured facts, achieving a higher F1 score (~91%) and bear in mind, ensuring maximum real assaults were detected, including complex patterns like statistics injection and visitors manipulation.

8. Strengths and Weaknesses of Each Model

Random Forest is computationally green, interpretable, and effective for dependent, static information. However, it struggles with sequential dependencies, main to overlooked evolving assaults. On the opposite hand, LSTM excels in time-series information, taking pictures temporal styles and minimizing fake negatives. Its weaknesses lie in higher computational costs and decrease interpretability in comparison to RF.

9. Evaluation Metrics

Both fashions maintained high precision, reducing fake positives and unnecessary indicators. LSTM showed advanced consider, making sure minimal false negatives and detecting almost all actual assaults. The ROC and Precision-Recall curves showed LSTM's more potent capacity to address imbalanced datasets and distinguish between assault and regular interest effectively.

10. Real-World Implications

Random Forest is right for initial filtering and detecting simple, static assault patterns in low-latency environments. LSTM is important for dynamic, time-sensitive structures like IoT healthcare, in which tool behaviors evolve. Together, they form a robust detection framework capable of addressing diverse attack vectors, making sure complete protection.

11. Discussion

In this section, the results of the proposed Hybrid RF-LSTM model for cyber-assault detection in IoT healthcare structures are analyzed and in comparison with previous studies, observed by way of an interpretation of the findings.

11.1 Analysis of Results

The hybrid Random Forest (RF) and Long Short-Term Memory (LSTM) model performed a detection accuracy of 97%, surpassing the overall performance of man or woman fashions in the literature. Specifically, RF verified sturdy performance in dealing with static data, inclusive of network traffic and tool logs, attaining 94% accuracy in detecting unauthorized access and denial-of-service (DoS) assaults. In contrast, LSTM excelled in detecting time-structured anomalies, such as records injection assaults, reaching an F1 score of 91% and substantially reducing false negatives. The hybrid model progressed upon each by means of incorporating RF's precision in static anomaly detection and LSTM's functionality in handling time-series facts, accordingly leading to more comprehensive attack detection with minimum false positives or false negatives.

Compared to earlier research, the hybrid RF-LSTM method exhibited clean upgrades. [19] suggested an AUC of zero.95 for RF in detecting network-based totally assaults, at the same time [20] verified 93% accuracy for unauthorized get admission to detection the use of RF alone. The hybrid model provided a better common overall performance, improving detection accuracy and keep in mind, with 97% accuracy and 96% don't forget. This increase in performance demonstrates the gain of mixing static and sequential records processing for cyber-assault detection.

11.2 Comparison with Previous Studies

The results align with preceding works but display a high-quality enhancement inside the detection of each static and dynamic assault styles.

- RF [21] and LSTM [22] had been shown to perform nicely in detecting unique kinds of attacks, but each by myself has limitations:
  a. RF excels in identifying static attack patterns however struggles with time-collection facts.
  b. LSTM is fairly powerful for sequential records however faces demanding situations in coping with non-sequential, established statistics.

By combining these models, the hybrid technique mitigates the weaknesses of every character version, as evidenced through the advanced basic detection accuracy of ninety seven% carried out in this take a look at.

11.3 Interpretation of Results

The development in detection accuracy may be attributed to the complementary nature of RF and LSTM:

- RF's strength lies in its capability to handle high-dimensional records, together with network logs, in which styles of attack are frequently nicely-described and do no longer rely upon temporal sequences. This is vital for identifying commonplace assaults like DoS or unauthorized get entry to.
- LSTM's capacity to examine from sequential statistics permits it to capture the dynamic, evolving nature of attacks inclusive of data injection or site visitors manipulation, which often span over the years and require detection of diffused changes in behavior.

The reduction in false negatives is one of the most important outcomes of this have a look at. In healthcare IoT structures, lacking an assault could compromise affected person protection, making it important to locate all kinds of anomalies. By combining each fashion, the system performed close to-best consider, which guarantees that capability assaults are flagged as soon as they arise.

11.4 Personal Interpretation

The hybrid RF-LSTM version represents a full-size step forward in cybersecurity for healthcare IoT systems. The integration of two one of a kind device studying paradigms - RF for static patterns and LSTM for temporal statistics - proves relatively powerful for securing complicated IoT environments, which often require coping with both dependent records (e.g., logs) and time-series statistics (e.g., sensor readings).

In terms of real-world software, the potential of the hybrid version to minimize fake positives at the same time as ensuring high consider could significantly lessen the number of unnecessary alarms, which is a major issue in safety structures. False positives are costly, as they divert interest from actual threats, so ensuring minimal false alarms is crucial. Additionally, the hybrid machine's scalability makes it adaptable to various IoT healthcare gadgets, further growing its sensible applicability.

One area that calls for similarly investigation is the version's computational performance. While the modern-day gadget suggests precise performance, actual-time packages in healthcare require fashions to be now not simplest correct however additionally speedy and resource-green. Optimizing this hybrid version for actual-time deployment on gadgets with constrained computational power stays a essential next step.

12. Conclusion

The proposed cyber-attack detection machine leveraging Random Forest (RF) and Long Short-Term Memory (LSTM) demonstrates a sturdy and green solution for securing IoT healthcare environments. RF proved effective in detecting static anomalies with excessive accuracy and computational performance, making it appropriate for analyzing structured information which includes network site visitors and tool logs. On the opposite hand, LSTM excelled in shooting temporal dependencies, enabling the detection of evolving and complex threats, together with facts injection and site visitors manipulation attacks, with minimum fake negatives.

The integration of RF and LSTM right into a hybrid framework better the system's overall performance, accomplishing an universal detection accuracy of 97 %. This mixture addressed both static and sequential attack patterns, ensuring comprehensive danger detection in real-time. Furthermore, the hybrid version's scalability and adaptability make it a practical solution for dynamic IoT healthcare systems. Underscores the importance of mixing system getting to know and deep studying techniques to tackle the particular cybersecurity demanding situations in IoT healthcare. Future paintings should attention on incorporating adaptive learning mechanisms to cope with emerging threats and optimizing the model for large-scale deployment, making sure lengthy-term protection and resilience in vital healthcare infrastructures.

13. Future Work

The proposed device may be further developed with the aid of integrating adaptive gaining knowledge of techniques to decorate its potential to deal with emerging cyber threats, and by incorporating superior deep gaining knowledge of fashions, inclusive of interest-based totally networks, to improve its overall performance on complicated patterns. Additionally, blockchain era can be utilized to make certain statistics integrity and safety in healthcare environments. To allow deployment on aid-confined gadgets, strategies like model compression and side computing may be carried out. The system has to additionally be examined in actual-global environments in collaboration with healthcare companies, and its selection-making process may be stepped forward thru explainability gear like SHAP and LIME to growth transparency and believe.

References

[1] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, vol. 14, p. 100129, 2021, doi: https://doi.org/10.1016/j.iot.2019.100129

[2] A. Boukerche and R. Coutinho, "Design Guidelines for Machine Learning-based Cybersecurity in Internet of Things," *IEEE Network*, vol. 35, pp. 393-399, 2020, doi: http://dx.doi.org/10.1109/MNET.011.2000396

[3] F. Wu, C. Qiu, T. Wu, and M. R. Yuce, "Edge-based hybrid system implementation for long-range safety and healthcare IoT applications," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9970-9980, 2021, doi: https://doi.org/10.1109/JIOT.2021.3050445

[4] M. Waqas *et al.*, "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 4, p. e6662, 2022, doi: https://doi.org/10.1002/cpe.6662

[5] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST," *Computer Networks*, vol. 198, p. 108413, 2021, doi: https://doi.org/10.1016/j.comnet.2021.108413

[6] X. Wang, T. Liu, C. Feng, D. Fang, and X. Chen, "RF-CM: Cross-modal framework for rf-enabled few-shot human activity recognition," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 7, no. 1, pp. 1-28, 2023, doi: https://doi.org/10.1145/3580859

[7] Y. Zhang *et al.*, "Efficient and intelligent attack detection in software defined IoT networks," in *2020 IEEE International Conference on Embedded Software and Systems (ICESS)*, Shanghai, China, 2020: IEEE, pp. 1-9, doi: https://doi.org/10.1109/ICESS49830.2020.9301591

[8] S. Djaballah, L. Saidi, K. Meftah, A. Hechifa, M. Bajaj, and I. Zaitsev, "A hybrid LSTM random forest model with grey wolf optimization for enhanced detection of multiple bearing faults," *Scientific Reports*, vol. 14, p. 23997, 2024, doi: https://doi.org/10.1038/s41598-024-75174-x

[9] C. U. Om Kumar, J. Durairaj, S. A. Ahamed Ali, Y. Justindhas, and S. Marappan, "Effective intrusion detection system for IoT using optimized capsule auto encoder model," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 13, p. e6918, 2022, doi: https://doi.org/10.1002/cpe.6918

[10] W. Li, S. Vishwakarma, C. Tang, K. Woodbridge, R. J. Piechocki, and K. Chetty, "Using RF transmissions from IoT devices for occupancy detection and activity recognition," *IEEE Sensors Journal*, vol. 22, no. 3, pp. 2484-2495, 2021, doi: https://doi.org/10.1109/JSEN.2021.3134895

[11] A. K. Kalusivalingam, A. Sharma, N. Patel, and V. Singh, "Employing Random Forests and Long Short-Term Memory Networks for Enhanced Predictive Modeling of Disease Progression," *International Journal of AI and ML*, vol. 2, no. 3, 2021

[12] B. Barnes-Cook and T. O'Shea, "Scalable wireless anomaly detection with generative-LSTMs on RF post-detection metadata," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, Austin, TX, USA, 2022: IEEE, pp. 483-488, doi: https://doi.org/10.1109/WCNC51071.2022.9771754

[13] N. Varshney, P. Madan, A. Shrivastava, A. P. Srivastava, C. P. KUMAR, and K. Khan, "Real-Time Anomaly Detection in IoT Healthcare Devices With LSTM," in *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2023, vol. 1: IEEE, pp. 1-6, doi: https://doi.org/10.1109/ICAIIHI57871.2023.10489823

[14] I. A. Kandhro *et al.*, "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEE Access*, vol. 11, pp. 9136-9148, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3238664

[15] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari, and M. Almutiry, "A hybrid deep learning approach for bottleneck detection in IoT," *IEEE Access*, vol. 10, pp. 77039-77053, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3188635

[16] M. K. Saeed, A. Al Mazroa, B. M. Alghamdi, F. S. Alallah, A. Alshareef, and A. Mahmud, "Predictive analytics of complex healthcare systems using deep learning based disease diagnosis model," *Scientific Reports*, vol. 14, p. 27497, 2024, doi: https://doi.org/10.1038/s41598-024-78015-z

[17] M. Al Razib, D. Javeed, M. T. Khan, R. Alkanhel, and M. S. A. Muthanna, "Cyber threats detection in smart environments using SDN-enabled DNN-LSTM hybrid framework," *IEEE Access*, vol. 10, pp. 53015-53026, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3172304

[18] N. Sun *et al.*, "Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748-1774, 2023, doi: https://doi.org/10.1109/COMST.2023.3273282

[19] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, "Comparative evaluation of ai-based techniques for zero-day attacks detection," *Electronics*, vol. 11, no. 23, p. 3934, 2022, doi: https://doi.org/10.3390/electronics11233934

[20] W. Ding and H. Sun, "Prediction of PM2. 5 concentration based on the weighted RF-LSTM model," *Earth Science Informatics*, vol. 16, pp. 3023-3037, 2023, doi: https://doi.org/10.1007/s12145-023-01111-7

[21] M. Almehdhar *et al.*, "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 869-906, 2024, doi: https://doi.org/10.1109/OJVT.2024.3422253

[22] F. Zahra, N. Jhanjhi, N. Khan, S. N. Brohi, M. Masud, and S. Aljahdali, "Protocol-specific and sensor network-inherited attack detection in IoT using machine learning," *Applied Sciences*, vol. 12, no. 22, p. 11598, 2022, doi: https://doi.org/10.3390/app122211598

How to cite this article

A. A. Hammad, " Random Forest and LSTM Hybrid Model for Detecting DDoS Attacks in Healthcare IoT Networks," *CyberSystem J.*, vol. 1, no. 2, pp. 1-8, 2024. doi: 10.57238/csj.0kdtzj06

Access this article online