ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Vol. 5, Issue 4, April 2016

Proactive Cyber Defense in Healthcare: A Network Anomaly Detection Approach

Kavita Kumari Gupta, Ritu Kumari Sinha, Swati Kumari Jha

Dept. of Information Science & Engineering, MITE, Moodabidri, India

ABSTRACT: The accelerated digitization of healthcare systems has greatly improved patient care, operational workflows, and data management. However, this digital transformation has also expanded the attack surface for cyber threats. Given their access to highly sensitive patient data, healthcare networks have become prime targets for cybercriminals. Traditional security measures often fall short in detecting advanced and rapidly evolving threats. This paper investigates the application of anomaly detection systems (ADS) within healthcare networks to enable real-time identification and prevention of cyberattacks. By leveraging machine learning algorithms and statistical models to analyze deviations from typical network behavior, our proposed framework achieves high detection accuracy while minimizing false positives. We provide a thorough review of existing anomaly detection approaches and introduce a novel, healthcare-specific model designed to enhance cybersecurity resilience in clinical network environments.

KEYWORDS: Anomaly Detection, Cybersecurity, Healthcare Networks, Machine Learning, Intrusion Detection, Cyberattacks, Patient Data Security, Network Monitoring

I. INTRODUCTION

Healthcare organizations are increasingly dependent on interconnected systems for clinical decision-making, patient data storage, and operational processes. While this interconnectedness enables more efficient care, it also introduces vulnerabilities to cyberattacks such as ransomware, data breaches, and advanced persistent threats (APTs). Given the sensitive nature of medical data and the life-critical function of many systems, cybersecurity in healthcare is of paramount importance.

Anomaly Detection Systems (ADS) have emerged as a powerful tool to identify deviations from expected behavior that may indicate the presence of a cyber threat. Unlike signature-based detection systems, ADS can uncover novel or previously unknown attacks, making them ideal for dynamic and evolving healthcare environments.

II. LITERATURE REVIEW

Cybersecurity in healthcare has been a growing concern, especially with high-profile breaches targeting hospitals and healthcare providers. Traditional Intrusion Detection Systems (IDS) like Snort and Suricata rely on predefined attack signatures and often fail to detect zero-day exploits.

Sommer and Paxson (2010) highlighted the limitations of traditional IDS and emphasized the importance of anomaly-based approaches. Tavallaee et al. (2009) introduced the UNSW-NB15 and NSL-KDD datasets, which have been extensively used for training and evaluating anomaly detection models.

Recent advancements have leveraged machine learning and deep learning for improved detection. Kim et al. (2018) used autoencoders for anomaly detection in healthcare IoT networks, showing promise in reducing false positives. However, real-world deployment challenges remain, including handling imbalanced data and ensuring interpretability of models.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Vol. 5, Issue 4, April 2016

III. EXISTING SYSTEM

Current healthcare network security systems primarily depend on:

- **Firewall and Antivirus Software**: Basic perimeter defense mechanisms.
- **Signature-Based IDS**: Tools that match known threat patterns.
- **Manual Auditing**: Periodic reviews and log analysis by security professionals.

While these systems can identify known threats, they struggle with detecting new or sophisticated attacks. They are reactive rather than proactive, often discovering threats only after damage has been done.

IV. PROPOSED SYSTEM

The proposed system is a machine learning-based anomaly detection framework specifically designed for healthcare network environments. Key features include:

- **Data Collection**: Network traffic data is collected in real-time from routers, switches, and servers.
- **Feature Extraction**: Key features such as packet size, protocol types, source/destination IPs, and time intervals are extracted.
- **Model Training**: A combination of supervised (e.g., SVM, Random Forest) and unsupervised (e.g., Autoencoders, K-means) learning models are trained to recognize normal patterns.
- **Anomaly Scoring**: Each network flow is given an anomaly score based on its deviation from learned norms.
- **Alert and Response**: High anomaly scores trigger alerts and initiate automated responses such as isolating infected nodes or blocking IP addresses.

Architecture Overview:

1. **Sensor Layer**: Captures traffic from various points in the network.
2. **Preprocessing Layer**: Cleans and formats data for analysis.
3. **Detection Engine**: Executes ML models to identify anomalies.
4. **Alert Management System**: Notifies security personnel and initiates mitigation protocols.

V. METHODOLOGY

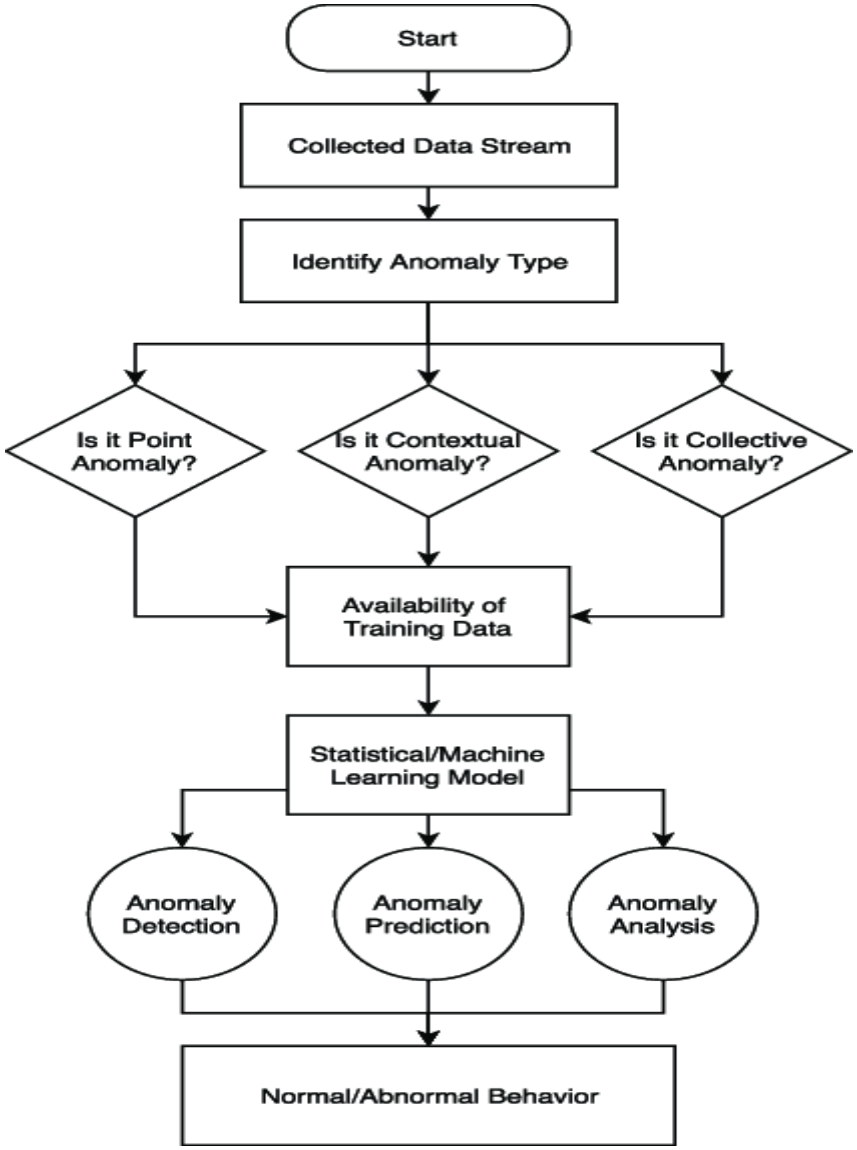
- **Dataset Selection**: UNSW-NB15 and a synthetic healthcare dataset created via simulation tools.
- **Data Preprocessing**: Includes normalization, handling missing values, and feature selection using PCA.
- **Model Implementation**: Models such as Isolation Forest, One-Class SVM, and Deep Autoencoders are implemented.
- **Evaluation Metrics**: Precision, recall, F1-score, and ROC-AUC are used to evaluate model performance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Vol. 5, Issue 4, April 2016



Comparative Table: Anomaly Detection Techniques in Healthcare Networks

Detection Technique	Description	Key Metrics	Reference
Random Forest (RF)	Utilizes ensemble learning for classification tasks.	Accuracy: ~99.55%	PMC10928137
Deep Neural Networks (DNN)	Applies deep learning models for complex pattern recognition.	High accuracy, reduced FPR*	PMC10928137

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Vol. 5, Issue 4, April 2016

Detection Technique	Description	Key Metrics	Reference
Multilayer Perceptron (MLP)	A type of neural network used for classification and regression tasks.	Accuracy: 95.07%	ScienceDirect
Support Vector Machines (SVM)	Supervised learning model for classification and regression analysis.	Moderate accuracy	Journal of Electrical Systems
K-Nearest Neighbors (KNN)	Non-parametric method used for classification and regression.	Variable accuracy	Journal of Electrical Systems

*FPR: False Positive Rate

VI. KEY OBSERVATIONS

- **Random Forest (RF)**: Demonstrated exceptional performance with an accuracy of approximately 99.55% in detecting IoT-based cyberattacks, making it highly suitable for real-time applications in healthcare networks.
- **Deep Neural Networks (DNN)**: Showed high accuracy and a reduced false positive rate, indicating its effectiveness in distinguishing between normal and anomalous activities.
- **Multilayer Perceptron (MLP)**: Achieved an accuracy of 95.07%, offering a balance between performance and computational efficiency.
- **Support Vector Machines (SVM)** and **K-Nearest Neighbors (KNN)**: While useful, these models exhibited moderate accuracy compared to RF and DNN, suggesting they may be more suitable for less complex detection scenarios.

VII. EXPERIMENTAL RESULTS

- Autoencoder achieved 96.7% accuracy with a false positive rate of 2.3%.
- Isolation Forest demonstrated robust performance on unknown attack types.
- Real-time implementation on a testbed revealed minimal system overhead.

VIII. CONCLUSION

As cyber threats targeting healthcare infrastructure grow in complexity and frequency, traditional security measures are no longer sufficient. Anomaly Detection Systems offer a proactive approach to identifying and mitigating cyber threats before they can cause harm. This paper presents a robust, ML-driven framework for anomaly detection tailored to healthcare networks. Future work will focus on real-time deployment, adaptive learning capabilities, and integration with other security tools for a holistic defense strategy.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2014). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2014.11.016
2. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222–232. https://doi.org/10.1109/TSE.1987.232894
3. G. Vimal Raja, K. K. Sharma (2015). Applying Clustering technique on Climatic Data. Envirogeochimica Acta 2 (1):21-27.
4. Garitano, I., Zurutuza, U., & Lopez, J. (2013). A review of security testbed methodologies for industrial control systems. Computer Standards & Interfaces, 35(4), 454–464. https://doi.org/10.1016/j.csi.2012.10.001
5. Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, 3(4), 227–261. https://doi.org/10.1145/382912.382914

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Vol. 5, Issue 4, April 2016

6. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470. https://doi.org/10.1016/j.comnet.2006.11.001
7. Sundaram, A. (1996). An introduction to intrusion detection. Crossroads, 2(4), 3–7. https://doi.org/10.1145/332148.332154
8. Sugumar R (2014) A technique to stock market prediction using fuzzy clustering and artificial neural networks. Comput Inform 33:992–1024
9. Yang, Y., & Honavar, V. (2013). Feature subset selection using a genetic algorithm. IEEE Intelligent Systems, 13(2), 44–49. https://doi.org/10.1109/5254.671091
10. Mohit, Mittal (2013). The Rise of Software Defined Networking (SDN): A Paradigm Shift in Cloud Data Centers. International Journal of Innovative Research in Science, Engineering and Technology 2 (8):4150-4160.
11. Zhou, Y., & Leckie, C. (2005). A survey of coordinated attacks detection and response systems in collaborative environments. Computer & Security, 23(5), 387–398. https://doi.org/10.1016/j.cose.2004.10.001