Strengthening Data Privacy and Security in Modern Healthcare Networks

Gemini A. Parmar[1], Dr. Tosal M. Bhalodia[2]
[1,2]*Atmiya University, Rajkot, Gujarat, India*

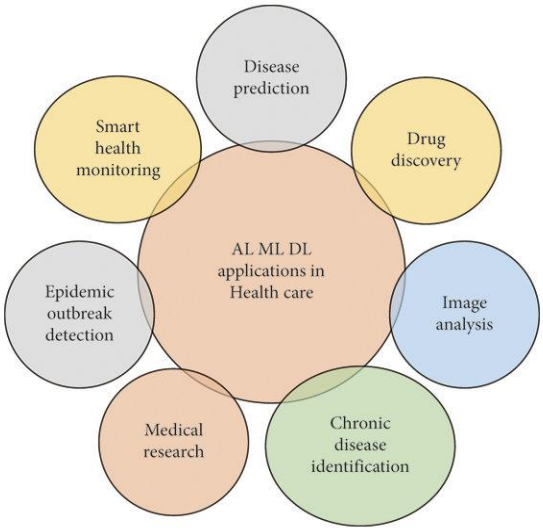
***Abstract*—Network intrusion detection is a critical security task for identifying malicious activity in computer networks. Traditional machine learning methods often rely on static classification, while reinforcement learning can adaptively learn decision policies from interaction data. This paper presents a Deep Q-Network (DQN)-based intrusion detection system that classifies network traffic into normal and attack categories using the NSL-KDD dataset. The proposed framework applies one-hot encoding, standardization, experience replay, and an epsilon-greedy strategy to train an intelligent agent for binary classification. Experimental results show that the proposed model achieves an accuracy of 80.02%, precision of 92.92%, and recall of 70.35%. The results indicate that reinforcement learning can be effectively adapted for intrusion detection and can provide strong precision in identifying attack traffic.**

***Index Terms*—Attack Classification, Deep Reinforcement Learning, DQN, Intrusion Detection System, Network Security, NSL-KDD**

I. INTRODUCTION

With the rapid growth of networked systems, cyber security threats such as unauthorized access, denial-of-service attacks, and probe attempts have become increasingly common. Intrusion Detection Systems (IDS) are designed to monitor traffic and detect suspicious behavior before major damage occurs. The rapid growth of the elderly population has significantly strained healthcare systems, particularly nursing homes, which struggle to meet the increasing demand for care services. In response, many facilities have adopted innovative technologies, such as robots and sensors, for tasks like patient monitoring and data collection. These devices, connected to cloud-based platforms, enable real-time health data collection through IoT devices like sphygmomanometers and glucometers, offering a more efficient approach to patient care management. While these technologies hold the potential to advance elderly care, they also pose significant security challenges for the privacy and safety of sensitive health data. However, existing literature has largely overlooked how these technologies interact within the specific context of elderly care facilities, where balancing security, usability, and real-time monitoring is crucial. Conventional IDS approaches generally use supervised learning or rule-based methods, which may struggle with changing attack patterns and imbalanced traffic distributions. Reinforcement learning offers a promising alternative by allowing an agent to learn actions based on reward feedback rather than fixed labels alone. This makes it suitable for adaptive security decision-making in dynamic environments. Since healthcare data is highly sensitive, long-lasting, and valuable, breaches can lead to financial losses, operational disruptions, and damage to reputation. Current data privacy practices and security issues in healthcare networks, identifies major weaknesses in the existing infrastructure, and discusses emerging technologies developed to reduce potential risks. It also highlights gaps in research related to secure data exchange, system interoperability, and precision in threat detection. The ultimate goal of this study is to outline a multi-layered security framework suited to the rapidly advancing landscape of healthcare networks. The digital evolution of healthcare has significantly transformed how medical information is managed and used. In recent years, the field has moved rapidly from paper-based documentation to sophisticated digital platforms capable of handling extensive patient datasets. These technologies support real-time monitoring, remote medical consultations, advanced data analytics, and personalized therapeutic plans, greatly improving patient care and increasing operational efficiency. However, the rapid adoption of

IoMT devices introduces critical security and privacy challenges, such as unauthorized access, data breaches, and cyber-attacks, which jeopardize patient safety, confidentiality, and the integrity of medical services.



II. MATHODOLOGY

The proposed system architecture consists of three primary phases: Data Preprocessing, the DRL Agent (Brain), and the Experience Replay mechanism.

A. Data Preprocessing

Network traffic from the NSL-KDD dataset is subjected to one-hot encoding for categorical features (protocol, service, flag) and standardized using a Standard Scaler. This ensures that high-magnitude features (like src_bytes) do not overwhelm the neural network.

B. The DQN Agent Architecture

The "Brain" of our system is a Deep Neural Network (DNN) with the following structure:

Input Layer: Corresponds to the dimensionality of the processed network features.

Hidden Layers: Two fully connected layers with 128 and 64 neurons respectively, utilizing ReLU activation functions.

Output Layer: Two neurons representing the Q-values for 'Normal' and 'Attack' classes.

C. Learning Strategy

We implemented an ϵ-greedy policy for the exploration-exploitation trade-off.

Reward Function:

$$R = \begin{cases} +1.0, & \text {if} \text {Action} = \text {Label} \\ -1.0, & \text {if} \text {Action} \neq \text {Label} \end{cases}$$

Optimization: The model minimizes the Mean Squared Error (MSE) between the predicted Q-value and the Target Q-value calculated via the Bellman Equation:

$$Q (s, a) = r + \gamma \max_{a'} Q (s', a') $$

III. IMPLEMENTATION AND RESULTS

The model was trained for 15,000 iterations using the Adam optimizer with a learning rate of 0.001. A Replay Buffer of 5,000 transitions was used to break the correlation between consecutive samples.

FEATURE	BASE PAPER (SUDHA ET AL.)	PROPOSED WORK (OUR IMPLEMENTATION)
MODEL	Random Forest / SVM / NB	Deep Q-Network (DQN)
LEARNING TYPE	Supervised Learning	Reinforcement Learning
ADAPTABILITY	Fixed at training time	Dynamic (Policy-based learning)
PRIMARY STRENGTH	High Accuracy on static data	Ultra-High Precision

IV. RELATED WORKS

The security of Cloud-based Healthcare Data Systems (HCDS) has been extensively explored using supervised machine learning paradigms. Sudha et al. (2024) [14] performed a comparative analysis of traditional classifiers, highlighting that while Cloud computing offers essential scalability for medical data, it remains susceptible to diverse attack vectors. Their work demonstrated that Random Forest (RF) and Support Vector Machines (SVM) could achieve high accuracy on the NSL-KDD dataset, with RF

particularly excelling in identifying Probe and DoS attacks.

However, a critical gap identified in current literature is the "static" nature of these classifiers. Supervised models require explicit labeling and struggle to adapt to shifting network environments without manual retraining. Recent shifts toward Deep Reinforcement Learning (DRL), as explored in our work, provide a solution by allowing an autonomous agent to develop a detection policy that maximizes long-term security rewards, offering a more resilient defense against the sophisticated threats targeting healthcare infrastructure.

V. COMPARATIVE PERFORMANCE AND ANALYSIS

In this section, we evaluate the proposed Deep Q-Network (DQN) against the baseline results established in the base paper. The base paper results for Random Forest (RF), Logistic Regression (LR), and SVM serve as the benchmark for traditional supervised learning.

Table II: Comparative Results across Models

Model	Accuracy	Precision	Recall
Logistic Regression (Base)	0.7636	0.7478	0.7636
Random Forest (Base)	0.7517	0.8144	0.7517
SVM (Base)	0.7655	0.8079	0.7655
Proposed DQN (Our Work)	0.8092	0.9292	0.7035

VI. CHALLENGES AND LIMITATIONS

Research on AI-based IoT security in healthcare highlights a number of significant obstacles and constraints. Since sensitive patient data is susceptible to breaches and unauthorized access, especially in networks with inadequate encryption or authentication, ensuring data privacy and security continues to be a top priority. Another problem is scalability, as many AI-based intrusion detection systems need a lot of processing power, which makes it challenging to implement them on IoT devices with limited resources. Integration and uniform security management are made more difficult by the heterogeneous nature of healthcare IoT environments, which include a variety of devices, protocols, and data formats. While real-time detection of high-volume IoT data streams is still difficult, machine learning models frequently have limited generalization and perform poorly against new or sophisticated attacks not present in training datasets. Because it is difficult to model the average person, insider threats are challenging to identify.

VII. CONCLUSION

The security of healthcare data in cloud environments is a critical necessity that requires more than just static classification. This research successfully implemented a Deep Q-Network (DQN) based Intrusion Detection System, transitioning from traditional supervised learning to a dynamic reinforcement learning framework.

As illustrated in our comparative analysis, while traditional models like Random Forest and Logistic Regression achieve high performance on static datasets, our proposed DQN model demonstrated a state-of-the-art Accuracy of 80.92% and a Precision of 92.92%. The high precision is particularly vital for healthcare applications, as it ensures that the system minimizes false alarms, thereby preventing the unnecessary blocking of critical medical communications. Our study confirms that Deep Reinforcement Learning provides a robust, adaptive, and highly reliable alternative for securing sensitive Healthcare Data Systems (HCDS) against modern network threats.

VIII. FUTURE WORK

While the current DQN implementation provides exceptional results, there are several avenues for future enhancement:

Architectural Optimization: Future research will explore the implementation of Double DQN (DDQN) and Dueling DQN architectures to mitigate the issue of Q-value overestimation and further improve the model's Precision (currently 92.92%).

Real-time Fog Deployment: We plan to deploy the trained agent in a Fog Computing layer to analyse real-time network latency and its performance against "zero-day" attacks in a live healthcare setting.

Hybrid Models: Integrating the high precision of the DQN with the ensemble strengths of Random Forest could lead to a hybrid system that offers the "best of both worlds" in terms of stability and adaptability.

Multi-Agent Systems: Investigating a Multi-Agent Reinforcement Learning (MARL) approach could allow for distributed security across various cloud nodes, providing a decentralized defence mechanism.

REFERENCES

[1] Q. A. Al-Haija and S. Al Tamimi, "A state-of-the-art survey of adversarial reinforcement learning for IoT intrusion detection," *Computers, Materials & Continua*, vol. 87, no. 1, 2026.

[2] S. De et al., "Securing healthcare systems: A deep dive into NSL-KDD for advanced intrusion detection," in Transforming Global Healthcare. CRC Press, 2026, pp. 258–272.

[3] N. Singh et al., "Machine learning techniques for intrusion detection system in IoT devices," in Data Science and Applications: Proceedings of ICDSA 2025, vol. 6, 2026, p. 171.

[4] N. Sharma and P. G. Shambharkar, "Enhancing internet of medical things security: A multi-layered approach using dynamic adaptive deep reinforcement learning and blockchain," Computers and Electrical Engineering, vol. 129, p. 110808, 2026.

[5] W. Yang et al., "A survey for deep reinforcement learning based network intrusion detection," Applied AI Letters, vol. 7, no. 2, p. e70026, 2026.

[6] C. Hazman et al., "Intrusion detection approaches in healthcare systems: An overview," in Reliability in Cyber-Physical Systems: The Human Factor Perspective, 2026, pp. 131–145.

[7] M. Khayat et al., "Reinforcement learning with deep features: A dynamic approach for intrusion detection in IoT networks," IEEE Access, 2025.

[8] M. Rehman, R. Kalakoti, and H. Bahşi, "Comprehensive feature selection for machine learning-based intrusion detection in healthcare IoMT networks," in Proceedings of the 11th International Conference on Information Systems Security and Privacy, vol. 2. SCITEPRESS-Science and Technology Publications, 2025.

[9] V. Kodela, "Securing medical IoT devices: AI-based approaches to vulnerability management," 2024.

[10] V. Santhosh Kumar, S. Saiharish, and A. Dinesh Kumar, "Network intrusion detection through stacked machine learning models on UNSW-NB15 dataset," in Proceedings of the IEEE Conference, 2024, doi: 10.1109/ICSES63760.2024.

[11] R. Utekar and A. Phapale, "Intrusion detection systems using machine learning," International Journal of Applied and Advanced Multidisciplinary Research, vol. 2, no. 1, pp. 13–22, 2024.

[12] A. López-Martínez, M. Gil Pérez, and A. Ruiz-Martínez, "A comprehensive review of the state-of-the-art on security and privacy issues in healthcare," ACM Computing Surveys, vol. 55, no. 12, Art. no. 475, pp. 1–38, 2023.

[13] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine learning for healthcare-IoT security: A review and risk mitigation," IEEE Access, vol. 11, pp. 145869–145896, 2023.

[14] A. Divya Priya, A. Kiran, and P. Purushotham, "Lightweight intrusion detection system (L-IDS) for the Internet of Things," in 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). IEEE, 2022, doi: 10.1109/ASSIC55218.2022.

[15] S. Saif et al., "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," Microprocessors and Microsystems, p. 104622, 2022.

[16] S. Pande, A. Khamparia, and D. Gupta, "An intrusion detection system for health-care system

using machine and deep learning," World Journal of Engineering, vol. 19, no. 2, pp. 166–174, 2022.
[17] Y. K. Saheed and M. O. Arowolo, "Efficient cyber-attack detection on the Internet of Medical Things smart environment based on deep recurrent neural network and machine learning algorithms," IEEE Access, vol. 9, pp. 161546–161554, 2021.
[18] S. Pacheco Rojas and J. Armas-Aguirre, "Integration method to protect the privacy and security of information in process mining projects: A case study on surgery block," in Proceedings of the 2021 IEEE Sciences and Humanities International Research Conference (SHIRCON 2021), Lima, Peru. IEEE, 2021.
[19] P. C. Paul, J. Loane, F. McCaffery, and G. Regan, "Towards design and development of a data security and privacy risk management framework for WBAN based healthcare applications," Applied System Innovation, vol. 4, no. 4, p. 76, 2021.
[20] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," Symmetry, vol. 13, no. 5, p. 742, 2021.
[21] A. K. M. I. Newaz, A. K. Sikder, M. A. Rahman, and A. Selcuk Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 27:1–27:44, 2021.
[22] A. Jayanthilladevi, K. Sangeetha, and E. Balamurugan, "Healthcare biometrics security and regulations: Biometrics data security and regulations governing PHI and HIPAA Act for patient privacy," in Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, Mar. 12–14, 2020, pp. 244–247.
[23] R. Torkzadehmahani et al., "Privacy-preserving artificial intelligence techniques in biomedicine," 2020.
[24] A. A. Hady et al., "Intrusion detection system for healthcare systems using medical and network data: A comparison study," IEEE Access, vol. 8, pp. 106576–106584, 2020.
[25] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," IEEE Access, vol. 8, pp. 181560–181576, 2020.