JOURNAL OF MULTIDISCIPLINARY RESEARCH AND INTEGRATED SCIENCES

Volume 2, Issue 1, 2022 | **Article ID:** JMRIS-2022-003 | **Pages:** 25-37 | **Article Type:** Systematic Technical Review
Received: 01-02-2022 | **Revised:** 12-02-2022 | **Accepted:** 28-02-2022 | **Published:** 15-03-2022

Comparative Performance of Machine-Learning Algorithms for Detecting Network Intrusions in Internet-of-Medical-Things Environments: A Systematic Technical Evidence Synthesis

Thomas Hughes[1*]

[1] *National University of Singapore, Singapore*

***Corresponding author:** Thomas Hughes, National University of Singapore, Singapore | tomh124@gmail.com.

ABSTRACT

Background: The Internet of Medical Things (IoMT) connects wearable sensors, bedside monitors, implantable devices, gateways, clinical systems and cloud infrastructure. Although connectivity supports continuous monitoring and more efficient healthcare delivery, it also introduces network attack surfaces capable of affecting confidentiality, integrity, availability and potentially patient safety. Machine-learning-based intrusion detection systems (IDSs) have therefore received increasing attention. **Objective:** To compare machine-learning approaches available through 2021 for detecting network intrusions in IoMT environments and identify algorithmic and deployment characteristics most appropriate for healthcare networks. **Methods:** A structured technical evidence synthesis was conducted using peer-reviewed studies published no later than 31 December 2021. References were restricted to Q1 journals in cybersecurity, networking, artificial intelligence, Internet of Things and biomedical informatics. IoMT-specific studies were prioritized and supplemented with high-quality IoT intrusion-detection research where algorithms, datasets or methodological principles were directly transferable. Classical machine learning, ensemble learning and deep-learning approaches were compared across discrimination, multiclass detection, computational demand, interpretability, class imbalance, validation methodology and deployment feasibility. **Results:** Random Forest and related ensemble methods consistently demonstrated strong performance for structured network-flow data while retaining moderate computational and interpretive advantages. Deep belief networks and recurrent architectures demonstrated high detection performance for complex or sequential attack patterns. Hybrid CNN-LSTM models offered automatic feature learning and temporal modeling but required greater computational resources. A 2021 optimized deep recurrent approach reported 99.76% overall accuracy, while earlier IoMT studies demonstrated high detection performance using Random Forest, deep belief networks and ensemble architectures. However, direct ranking was inappropriate because studies used different datasets, attacks, feature sets and validation procedures. Dataset representativeness, class imbalance, false-alarm burden and computational location were at least as important as headline accuracy. **Conclusion:** No single algorithm can be considered universally optimal for IoMT intrusion detection. For structured flow-level data, Random Forest and ensemble methods provide a strong accuracy-efficiency compromise. Deep and recurrent architectures are attractive when temporal or high-dimensional attack patterns justify additional computational cost. Practical IoMT IDSs should employ layered deployment, per-class evaluation, temporally independent validation and explicit measurement of latency, false alarms and resource consumption.

Keywords: Internet of Medical Things; intrusion detection; machine learning; deep learning; Random Forest; cybersecurity; healthcare; network security; IoMT

1. Introduction

The Internet of Medical Things represents the integration of connected medical devices, sensors, communication networks and healthcare information infrastructure. Wearable physiological sensors, wireless body-area networks, bedside monitoring equipment, remote patient-monitoring devices and other connected clinical technologies can exchange data continuously.

These capabilities support remote care and real-time physiological monitoring but simultaneously expand the healthcare attack surface.

Unlike conventional enterprise computers, many medical and sensor devices possess constrained processors, limited memory, restricted battery capacity and long operational lifecycles. Security controls must therefore operate without substantially disrupting device functionality.

This challenge has encouraged development of network-based intrusion detection.

An IDS observes device or network activity and attempts to distinguish expected behavior from malicious activity. Traditional signature systems are effective when attack patterns are known in advance but can perform poorly when confronted with altered or previously unseen threats.

Machine learning provides an alternative by learning patterns from data.

Hady et al. demonstrated the feasibility of healthcare-specific intrusion detection by combining network and medical sensor information and comparing multiple machine-learning algorithms [1]. Thamilarasu et al. subsequently proposed a hierarchical mobile-agent IDS spanning wireless body-area networks and other connected medical devices [2]. Their framework used machine learning for network-level attacks while simultaneously monitoring abnormal sensor behavior.

Deep-learning approaches also emerged rapidly. Manimurugan et al. developed a deep belief neural network for IoMT attack detection and reported strong class-specific detection performance [3]. By 2021, ensemble fog-cloud and hybrid recurrent

architectures were being investigated as mechanisms for obtaining higher detection performance without transferring the complete computational burden to constrained medical devices [4-6].

The important question consequently shifted from whether machine learning can detect IoMT attacks to which type of machine-learning architecture is most appropriate for each IoMT security problem.

The present review aimed to compare classical, ensemble and deep-learning intrusion-detection approaches, determine the strengths and weaknesses of major algorithm families, evaluate factors affecting apparent model performance, identify appropriate performance metrics for healthcare deployment, and propose a layered model-selection and deployment strategy for IoMT environments.

2. Methods

2.1 Review Design

A structured technical evidence synthesis was performed using literature available through 31 December 2021.

Search concepts included combinations of:

Internet of Medical Things, IoMT, healthcare intrusion detection, machine learning, deep learning, Random Forest, ensemble learning, recurrent neural network, CNN-LSTM, cyberattack detection, network intrusion, and IoT security.

IoMT-specific experimental studies were prioritized. High-quality IoT studies and systematic surveys were included when their methodological findings directly informed medical-device network intrusion detection.

The evidence eligibility framework is summarised in Table 1.

2.2 Comparison Domains

Algorithms were evaluated across predictive discrimination, multiclass capability, computational complexity, memory requirements, feature-engineering dependence, temporal-learning capacity, interpretability, suitability for resource-constrained deployment, and reported validation quality.

Meta-analysis was not attempted because performance metrics were not derived from sufficiently homogeneous datasets or experimental conditions.

3. IoMT Threat Model

An IoMT network differs from a conventional office network because data communication can directly support diagnosis, monitoring or therapy.

An attack may therefore affect more than information confidentiality.

Potential consequences include interruption of physiological monitoring, manipulated sensor values, denial of medical-device availability, unauthorized network access, malware propagation, patient-data disclosure, and interference with clinical decision-making.

Healthcare 4.0 security reviews have consequently emphasized availability and integrity alongside conventional confidentiality requirements [7].

Major attack categories relevant to machine-learning IDSs include denial-of-service and distributed denial-of-service, botnet activity, scanning and reconnaissance, brute-force authentication, spoofing and impersonation, malware-related communication, data manipulation, and abnormal sensor/device behavior.

The goal of an IoMT IDS should therefore not be limited to a single binary decision.

A clinically useful system may need to distinguish multiple attack families while keeping false alarms sufficiently low for continuous operation.

4. Evidence From IoMT-Specific Studies

The principal pre-2022 Q1 IoMT intrusion-detection studies are summarised in Table 2.

Saheed and Arowolo's 2021 analysis is particularly informative because it explicitly compared deep recurrent and conventional supervised approaches and reported 99.76% accuracy for the proposed model [6].

Nevertheless, these figures must be interpreted cautiously.

The experiments differ in dataset composition, number of attack categories, feature preprocessing, class ratios, train-test division, attack-generation procedures, and whether the reported metric relates to binary or multiclass detection.

Thus, 99% accuracy in one experiment cannot automatically be interpreted as superior to 97% in another.

5. Classical Machine-Learning Algorithms

Traditional supervised algorithms remain highly relevant to IoMT security.

5.1 Decision Trees

Decision trees divide observations according to feature thresholds.

Advantages include low inference cost, intuitive rules, limited preprocessing requirements, and straightforward explanation.

Their primary weakness is susceptibility to overfitting.

Small changes in training observations can generate substantially different trees.

For resource-sensitive applications, however, compact trees may remain attractive.

5.2 Random Forest

Random Forest combines multiple decision trees trained on resampled data and feature subsets.

Across IoT cybersecurity research, Random Forest repeatedly demonstrates strong performance on structured traffic features [1,2,9].

The algorithm offers several advantages nonlinear decision boundaries, automatic interaction modeling, resistance to individual-tree instability, limited scaling requirements, useful feature-importance measures, and comparatively efficient inference.

Hady et al.'s healthcare-specific comparative study found tree-based methods to be strong candidates for intrusion classification [1].

This is important because many IoMT IDS datasets consist primarily of tabular network-flow features—the type of data on which tree ensembles generally perform effectively.

5.3 Support Vector Machines

Support Vector Machines identify separating boundaries between classes and can model nonlinear relationships through kernel functions.

SVMs have historically performed well on intrusion-detection tasks but face potential limitations when training sets become very large, multiclass classification is required, frequent retraining is necessary, and interpretability is important.

Their inference cost may remain acceptable at gateway level, but scaling can become problematic compared with decision-tree approaches.

5.4 K-Nearest Neighbors

KNN provides conceptually simple instance-based classification.

Its main advantages are minimal training requirements and intuitive local classification.

However, inference requires comparison with stored observations, making latency and memory usage less attractive for high-volume network traffic.

KNN is consequently more appropriate as a benchmark than as the default architecture for large-scale IoMT monitoring.

6. Ensemble Learning

Ensemble learning combines multiple models to improve robustness.

Common approaches include bagging, boosting, voting, stacking, and heterogeneous ensembles.

Kumar et al. proposed an ensemble-learning and fog-cloud architecture specifically for IoMT cyberattack detection [4]. Their framework achieved high detection performance while distributing computation across fog-cloud infrastructure.

This architectural decision is important.

An IDS does not necessarily need to execute directly on the wearable sensor or medical device being protected.

Instead, a device-to-gateway-to-fog/edge-IDS-to-cloud/SOC architecture can permit use of more sophisticated models without exhausting endpoint resources.

7. Deep-Learning Approaches

7.1 Deep Belief Networks

Manimurugan et al. applied a deep belief neural network to IoMT attack classification [3].

Reported class-specific accuracies were approximately 99.37% for normal traffic, 97.93% for botnet, 97.71% for brute force, and 96.67% for DoS/DDoS traffic.

These findings demonstrate the ability of deep architectures to distinguish multiple classes.

However, model complexity and training burden are higher than for many conventional algorithms.

7.2 Recurrent Neural Networks

Network traffic has temporal characteristics.

A flow observed at one time point may become suspicious because of the sequence of events that preceded it.

Recurrent Neural Networks and Long Short-Term Memory networks explicitly model sequence dependencies.

Saheed and Arowolo used a deep recurrent architecture in an IoMT smart-environment context and reported 99.76% accuracy [6].

Their results support the use of temporal learning when attack patterns evolve across sequences rather than isolated observations.

7.3 Hybrid CNN-LSTM

Convolutional Neural Networks can extract local feature patterns, while LSTM networks capture temporal dependencies.

Khan and Akhunzada combined these capabilities in an SDN-enabled IoMT malware-detection system [5].

They compared CNN-LSTM with other hybrid deep-learning architectures using cross-validation and reported strong detection performance with favorable computational behavior.

Hybrid models are particularly attractive when raw or lightly processed data contain both local feature relationships and sequential structure.

Their disadvantage is increased architectural and tuning complexity.

8. Comparative Algorithm Assessment

The comparative machine-learning pipeline for network intrusion detection in IoMT environments is presented in Figure 1.

The practical comparison of principal algorithms is presented in Table 3.

The table highlights why a single universal ranking is inappropriate.

Random Forest may outperform a neural network on structured flow features while using far fewer computational resources.

Conversely, an LSTM may provide a meaningful advantage when the discriminative information is fundamentally temporal.

9. Feature Engineering

The quality of an IDS depends heavily on its representation of network behavior.

Important IoMT intrusion-detection feature groups are summarised in Table 4.

IoMT offers an additional opportunity unavailable to generic network IDSs: device context.

A glucose monitor, infusion pump and administrative workstation should not necessarily share the same normal-traffic profile.

Device-aware models may consequently reduce false positives.

10. Dataset Selection

Reported algorithm performance is only meaningful relative to the dataset on which it was measured.

Generic intrusion datasets are frequently used because they provide standardized labels.

However, IoMT communication differs from conventional enterprise traffic.

Relevant datasets should ideally contain medical-device communication, sensor traffic, wireless protocols, realistic benign device behavior, attack classes relevant to healthcare, and sufficient temporal diversity.

IoT-security literature has repeatedly identified dataset quality and representativeness as major research challenges [9-12].

Koroniotis et al.'s Bot-IoT work demonstrated the importance of building more realistic IoT botnet traffic rather than relying solely on legacy enterprise datasets [13].

A similar principle applies even more strongly to IoMT.

11. Class Imbalance

Network intrusion data are rarely balanced.

Some attacks may contain thousands of observations, while rare but clinically important attack types may appear infrequently.

Overall accuracy can therefore become misleading.

Consider a dataset containing 99,000 benign samples and 1,000 malicious samples.

A classifier predicting every observation as benign would achieve 99% accuracy while detecting zero attacks.

For this reason, IoMT IDS evaluation must report per-class performance.

The recommended performance measures are summarised in Table 5.

12. Why Accuracy Alone Is Insufficient

Many IoT intrusion-detection papers report accuracy above 95%.

Such results can appear impressive, but three questions must be asked.

First: What was the attack distribution?

Easy majority classes can dominate aggregate accuracy.

Second: How was the dataset divided?

Random splitting may distribute highly similar traffic from one attack session into both training and testing sets.

This can inflate performance.

Third: Was the test set collected later?

Attack behavior changes over time.

A real IDS predicts future network events, so chronological validation is more realistic than randomly mixing observations.

A strong design would therefore use a training period followed by a validation period and a later independent test period.

13. Computational Constraints

Deep-learning performance must be interpreted within the hardware constraints of IoMT.

A large neural model that produces a small increase in F1-score may be inappropriate if it significantly increases latency, memory use, battery consumption, and communication overhead.

Thamilarasu et al. explicitly designed their hierarchical architecture to obtain high detection performance while maintaining limited resource overhead [2].

Khan and Akhunzada similarly positioned intensive analysis within an SDN-enabled architecture rather than placing additional burden on constrained medical devices [5].

The appropriate location of the IDS is therefore part of algorithm selection.

14. Layered Deployment Architecture

The layered deployment strategy for machine-learning intrusion detection in IoMT is presented in Figure 2.

A four-level architecture is appropriate.

At Level 1, the medical-device layer, only lightweight local checks should be performed. Basic integrity monitoring, connection whitelisting, rate thresholds and authentication checks are appropriate at this level.

At Level 2, the edge or gateway layer can calculate flow features and run lightweight tree-based classifiers. This is an ideal location for Random Forest or compact ensemble models.

At Level 3, the fog or SDN controller has broader network visibility and more computational resources. Deep recurrent or ensemble architectures can operate here, and prior work supports the relevance of SDN orchestration for evolving IoMT threats [8].

At Level 4, the cloud or Security Operations Centre can perform model retraining, cross-device correlation, forensic analysis, threat-intelligence integration, and long-term anomaly modeling.

This layered structure avoids forcing one algorithm to solve every problem.

15. Recommended Comparative Experimental Design

A future study comparing algorithms should use the same dataset, preprocessing and splits for every model.

At minimum, the following should be compared logistic regression, Decision Tree, Random Forest, SVM, gradient boosting, multilayer neural network, LSTM, and CNN-LSTM.

All models should receive identical training and test samples.

Hyperparameter optimization should occur using the training data only.

The final test set must remain untouched until model selection is complete.

16. Feature Selection

More features do not necessarily improve an IDS.

Redundant features may increase training time, amplify noise, increase overfitting, complicate explanations, and increase deployment requirements.

Tree-based importance, mutual information or wrapper approaches can be used to reduce the feature set.

However, feature selection must occur inside cross-validation.

Selecting features using the complete dataset before test-set evaluation creates information leakage.

17. Binary Versus Multiclass Detection

Binary IDS models answer whether traffic is benign or malicious, whereas multiclass models identify what kind of malicious activity is occurring.

Binary classification is generally easier and can produce higher overall accuracy.

Therefore, results from binary and multiclass experiments should never be compared directly.

Healthcare networks benefit from multiclass identification because response differs according to attack type.

A scanning event may require investigation.

A DDoS attack may require immediate traffic mitigation.

A compromised medical device communicating with botnet infrastructure may require network isolation.

18. Interpretability

Machine-learning IDS outputs should provide sufficient explanation for security personnel.

Tree-based approaches possess an advantage because important features and decision pathways can be inspected relatively easily.

Deep networks are more difficult to interpret.

For healthcare systems, this distinction matters because automatically isolating a medical device can itself affect care.

An alert should therefore ideally provide predicted attack class, confidence/risk score, major abnormal features, affected device, destination/source, observed deviation, and recommended response.

Model interpretability becomes particularly important when security action can disrupt clinical workflow.

19. Discussion

The evidence available through 2021 demonstrates substantial progress in ML-based IoMT intrusion detection.

The strongest conclusion, however, is not that one algorithm consistently wins.

Instead, algorithm performance depends heavily on data representation and deployment context.

Classical tree-based algorithms remain highly competitive for network-flow data.

Random Forest in particular provides a favorable combination of nonlinear classification, robustness, manageable computational requirements, multiclass capability, and partial interpretability.

Deep learning becomes more attractive when feature relationships are complex or inherently sequential.

Deep belief networks demonstrated strong multiclass performance in IoMT attack detection [3], while recurrent and hybrid CNN-LSTM architectures extended detection toward temporal and automatically learned representations [5,6].

Ensemble models offer a third approach.

Kumar et al. combined ensemble learning with fog-cloud deployment, demonstrating the potential value of simultaneously considering classifier design and system architecture [4].

This is particularly important for IoMT because resource constraints fundamentally shape feasible cybersecurity solutions.

The resulting practical hierarchy is that structured tabular traffic with limited resources favors Random Forest or ensemble methods; complex nonlinear patterns favor boosting or deep learning; temporal attack behavior favors RNN/LSTM approaches; and

mixed spatial-temporal representations favor CNN-LSTM architectures.

This should be interpreted as a design framework rather than an absolute ranking.

20. Implications for Patient Safety

IoMT intrusion detection cannot be evaluated solely as a conventional IT-security problem.

False negatives can allow attacks to continue undetected.

However, false positives also have potential clinical consequences.

If an IDS incorrectly isolates a patient monitor, infusion-device gateway or other critical system, availability may be affected.

Healthcare IDS design must therefore optimize both attack detection and safe continuity of clinical service.

This favors graded responses.

For example, low-risk events may be logged only; intermediate-risk events may trigger enhanced monitoring and security review; high-risk events may prompt rate limiting or quarantine of non-critical traffic; and a critical confirmed attack may justify isolation of the affected endpoint according to clinical safety procedures.

21. Limitations

Several limitations should be acknowledged.

First, pre-2022 IoMT-specific machine-learning studies remained relatively limited compared with general IoT cybersecurity research.

Second, included studies used heterogeneous datasets and therefore could not support a statistically meaningful pooled algorithm ranking.

Third, many studies relied on simulated or benchmark traffic rather than long-term production hospital networks.

Fourth, aggregate accuracy was frequently emphasized despite class imbalance.

Fifth, model latency, energy consumption and memory requirements were reported less consistently than discrimination metrics.

Sixth, rapidly evolving threats create concept drift: a classifier trained on historical attacks may lose performance over time.

Finally, restriction to Q1 literature intentionally excluded some specialized IoMT security studies from lower-ranked journals and conference proceedings.

22. Future Research

Future research should move from isolated benchmark performance toward prospective IoMT validation.

Priority areas include multicentre medical-device traffic datasets, standardized attack definitions, temporal train-test separation, device-specific behavioral baselines, rare-attack evaluation, adversarial robustness, online/concept-drift adaptation, interpretable detection, federated or privacy-preserving learning, energy and latency measurement, and prospective deployment in hospital networks.

Research should also evaluate whether combining network features with device-level physiological behavior improves detection.

A malicious packet stream may be easier to identify when the model understands what the medical device normally does.

23. Conclusion

Machine-learning-based intrusion detection offers substantial potential for securing Internet-of-Medical-Things networks.

Evidence available through 2021 demonstrates strong performance from classical machine learning, ensemble approaches and deep neural architectures.

However, no single algorithm can be considered universally superior.

Random Forest and ensemble methods provide a particularly strong compromise for structured network-flow data because they combine high predictive capacity with moderate computational requirements and reasonable interpretability.

Deep belief networks, RNNs and hybrid CNN-LSTM architectures become attractive where attack characteristics involve complex nonlinear or temporal dependencies.

Model selection should therefore be driven not by headline accuracy but by attack coverage, per-class recall, false-positive burden, computational cost, inference latency, dataset realism and temporal generalization.

For IoMT specifically, architecture matters as much as algorithm choice.

A layered IDS that places lightweight detection near medical devices and computationally intensive analysis at gateway, fog, SDN or cloud layers provides a practical strategy for reconciling security performance with resource constraints.

Future IoMT cybersecurity research should consequently shift from asking which classifier produces the highest laboratory accuracy toward determining which detection system remains accurate, efficient, interpretable and clinically safe when confronted with evolving attacks in real healthcare networks.

Declarations

Author Contributions

The authors contributed to conceptualization, evidence synthesis, technical comparison, interpretation, manuscript preparation and critical revision.

Funding

No external funding was received.

Ethical Approval

Not applicable. This study synthesized previously published technical evidence and did not involve human participants or patient-level data.

Consent to Participate

Not applicable.

Data Availability

No novel dataset was generated or analyzed.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Hady AA, Ghubaish A, Salman T, Unal D, Jain R. Intrusion detection system for healthcare systems using medical and network data: a comparison study. IEEE Access. 2020;8:106576-106584. doi:10.1109/ACCESS.2020.3000421.
2. Thamilarasu G, Odesile A, Hoang A. An intrusion detection system for Internet of Medical Things. IEEE Access. 2020;8:181560-181576. doi:10.1109/ACCESS.2020.3026260.
3. Manimurugan S, Al-Mutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, Patan R. Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network. IEEE Access. 2020;8:77396-77404. doi:10.1109/ACCESS.2020.2986013.
4. Kumar P, Gupta GP, Tripathi R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput Commun. 2021;166:110-124.
5. Khan S, Akhunzada A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Comput Commun. 2021;170:209-216. doi:10.1016/j.comcom.2021.01.013.

6. Saheed YK, Arowolo MO. Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access. 2021;9:161546-161554. doi:10.1109/ACCESS.2021.3128837.

7. Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput Commun. 2020;153:311-335. doi:10.1016/j.comcom.2020.02.018.

8. Liaqat S, Akhunzada A, Shaikh FS, Giannetsos A, Jan MA. SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). Comput Commun. 2020;160:697-705. doi:10.1016/j.comcom.2020.07.006.

9. Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Commun Surv Tutor. 2020;22(3):1646-1685.

10. Tahsien SM, Karimipour H, Spachos P. Machine learning based solutions for security of Internet of Things (IoT): a survey. J Netw Comput Appl. 2020;161:102630. doi:10.1016/j.jnca.2020.102630.

11. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. J Netw Comput Appl. 2017;84:25-37.

12. Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener Comput Syst. 2018;82:761-768.

13. Koroniotis N, Moustafa N, Sitnikova E, Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Gener Comput Syst. 2019;100:779-796.

14. Lohiya R, Thakkar A. Application domains, evaluation data sets, and research challenges of IoT: a systematic review. IEEE Internet Things J. 2021;8(11):8774-8798. doi:10.1109/JIOT.2020.3048439.

Table 1. Evidence eligibility framework

Domain	Inclusion criteria	Exclusion criteria
Publication date	≤31 December 2021	2022 onward
Journal quality	Q1 journal in relevant category	Lower-quartile or unranked source
Environment	IoMT, healthcare IoT or directly transferable IoT network	Unrelated enterprise-only security
Intervention	ML/DL-based network or device intrusion detection	Cryptography without IDS component
Outcomes	Accuracy, detection rate, precision, recall, F1, false alarms, efficiency	No quantitative or technical evaluation
Study type	Empirical study, systematic technical review	Editorial/opinion
Priority	Realistic or purpose-built IoMT evaluation	Generic benchmark without IoT relevance unless methodologically important

Table 2. Principal pre-2022 Q1 IoMT intrusion-detection studies

Study	Architecture	Principal contribution	Key implication
Hady et al. [1]	Comparative classical ML	Combined network traffic with healthcare/medical data	IoMT detection benefits from context beyond generic network features
Thamilarasu et al. [2]	Mobile-agent IDS + ML/regression	Hierarchical network- and device-level detection	Distributed architecture can reduce endpoint burden
Manimurugan et al. [3]	Deep belief neural network	Multiclass IoMT cyberattack detection	DL can model complex attack patterns
Kumar et al. [4]	Ensemble learning + fog-cloud	Distributed cyberattack-detection architecture	Fog processing can reduce dependence on constrained endpoints
Khan & Akhunzada [5]	Hybrid CNN-LSTM + SDN	Malware detection using spatial and temporal feature learning	Hybrid DL supports complex pattern recognition
Saheed & Arowolo [6]	Optimized DRNN + supervised ML	Comparative attack detection	Reported 99.76% overall accuracy for optimized approach
Liaqat et al. [8]	SDN orchestration + DL	Network-level orchestration against evolving IoMT threats	Centralized visibility can aid scalable detection

Table 3. Practical comparison of principal algorithms

Algorithm	Feature engineering	Temporal modeling	Interpretability	Computational demand	IoMT suitability
Logistic regression	High	No	Very high	Very low	Useful baseline
Decision Tree	Moderate	No	High	Low	Strong lightweight option
Random Forest	Moderate	No	Moderate-high	Low-moderate	Excellent for tabular network traffic
SVM	Moderate-high	No	Low-moderate	Moderate	Useful for moderate datasets
KNN	Moderate	No	Moderate	High inference cost	Limited large-scale use
Boosting ensemble	Moderate	No	Moderate	Moderate	Strong predictive option
Deep belief network	Low-moderate	Limited	Low	High	Strong complex classification
RNN/LSTM	Low-moderate	Yes	Low	High	Suitable for sequential attacks
CNN-LSTM	Low	Yes	Low	High	Strong for complex temporal patterns
Heterogeneous ensemble	Variable	Depends on members	Moderate-low	Moderate-high	High potential if properly validated

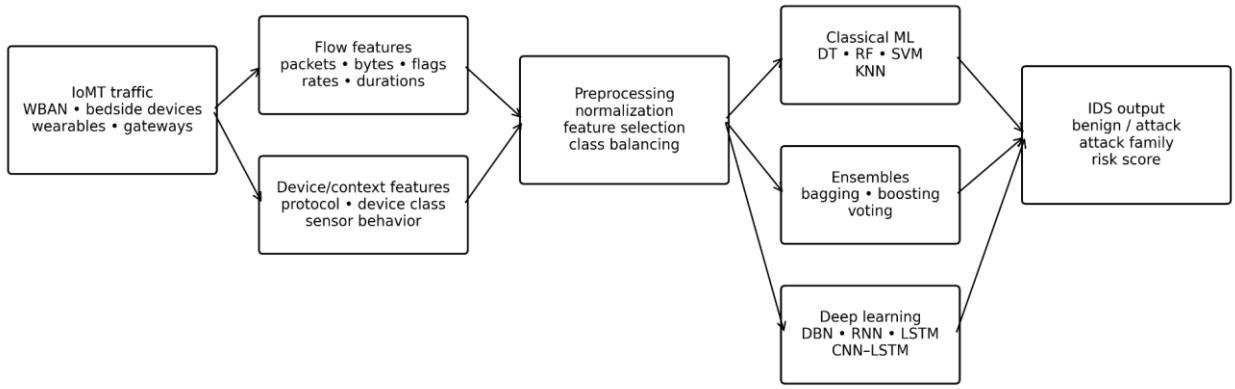
Table 4. Important IoMT intrusion-detection feature groups

Feature domain	Examples	Security relevance
Flow duration	Session duration	Abnormally long/short sessions
Packet volume	Packets sent/received	Flooding and scanning behavior
Byte volume	Incoming/outgoing bytes	Exfiltration or flooding
Packet rate	Packets/second	DoS/DDoS detection
Protocol	TCP, UDP, ICMP, application protocol	Attack-specific communication patterns
TCP flags	SYN, ACK, FIN, RST	Scanning/flooding indicators
Source/destination	Ports, endpoints	Service targeting
Inter-arrival timing	Packet timing statistics	Automated/bot behavior
Directionality	Upstream/downstream ratio	Device behavioral abnormality
Device identity	Device category/type	Context-sensitive baseline
Sensor behavior	Physiological data distribution	Device manipulation/anomaly detection
Historical sequence	Previous flows/events	Temporal intrusion identification

Table 5. Recommended performance measures

Metric	Purpose	Importance in IoMT
Accuracy	Overall classification correctness	Useful but inadequate alone
Recall/sensitivity	Proportion of attacks detected	Critical for patient-connected systems
Precision	Proportion of alerts that are genuine	Controls alert fatigue
F1-score	Balance of precision and recall	Useful under imbalance
Specificity	Correct benign classification	Measures unnecessary alerts
False-positive rate	Benign traffic incorrectly flagged	Operationally critical
MCC	Balanced binary/multiclass performance	Robust under imbalance
Per-class recall	Detection of individual attack types	Essential for rare attacks
Inference latency	Processing time	Required for real-time detection
Memory use	Deployment cost	Important for edge devices
CPU/energy demand	Resource burden	Important for IoMT gateways
Temporal validation	Performance on future traffic	Measures generalization

Figure 1. Comparative machine-learning pipeline for network intrusion detection in IoMT environments



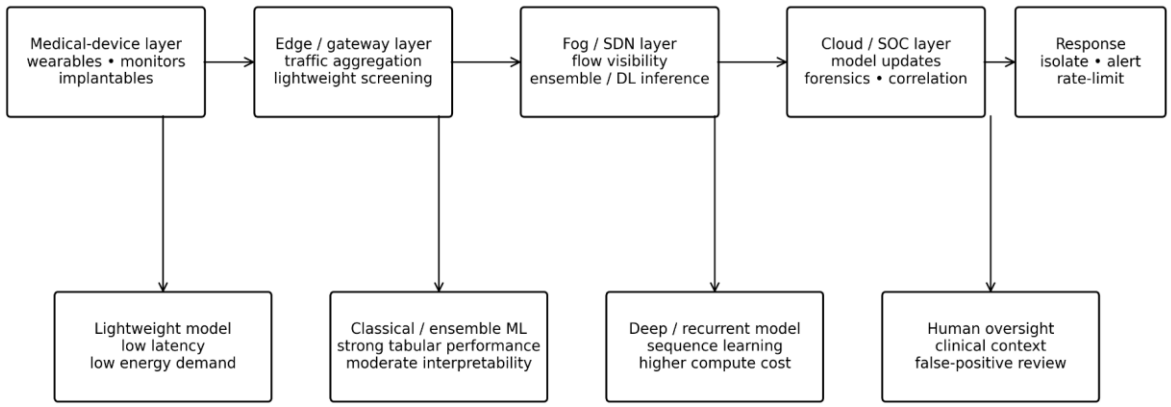
Evaluation must include: per-class recall • precision/F1 • false-alarm rate • MCC • latency • memory/CPU cost • external/temporal validation

Clinical constraint: detection must protect availability and patient safety without imposing excessive computation on resource-constrained medical devices.

Figure 1. Comparative machine-learning pipeline for network intrusion detection in IoMT environments.

Comparative intrusion-detection pipeline. The appropriate algorithm depends on input representation, attack objective, computational resources and required output. Evaluation should extend beyond aggregate accuracy.

Figure 2. Layered deployment strategy for machine-learning intrusion detection in IoMT



Recommended principle: place computation where resources and visibility are available; avoid making constrained patient-connected devices carry the full IDS burden.

Figure 2. Layered deployment strategy for machine-learning intrusion detection in IoMT.

Recommended layered architecture. Lightweight monitoring occurs close to devices, while increasingly computational models can operate at gateways, fog/SDN infrastructure or centralized security systems.

How to cite: Hughes T. (2022). Comparative Performance of Machine-Learning Algorithms for Detecting Network Intrusions in Internet-of-Medical-Things Environments: A Systematic Technical Evidence Synthesis. Journal of Multidisciplinary Research and Integrated Sciences, 2(1)

© 2022 Journal of Multidisciplinary Research and Integrated Sciences (JMRIS). Open access under CC BY 4.0.