Received October 23, 2025, accepted February 4, 2026, publication date for online-first April 9, 2026.

Original Research Article

Deep Learning Approach for Malware Classification and Threat Intelligence in Hospital Management

Md Mashfiquer Rahman[1,*], Md Mosiur Rahman[2], Sharmin Nahar[1], Md Mostafijur Rahman[1], Md Mostafizur Rahman[3], Md Shahadat Hossain[4]

[1] Department of Computer Science, Louisiana State University, Shreveport, LA, USA.
[2] Department of Computer Science & Engineering, Stamford University, Dhaka, Bangladesh.
[3] Department of Computer Science, San Francisco Bay University, San Francisco, CA, USA.
[4] Department of Computer Science, American International University, Dhaka, Bangladesh.
[*] Corresponding Author Email: mashfiq.cse@gmail.com

ABSTRACT

The growing dependence on digital systems in hospital administration has increased exposure to malware attacks, thereby jeopardizing patient safety and data integrity. To improve healthcare cybersecurity, this paper suggests a deep learning approach for malware classification and integrated threat intelligence. For feature extraction, convolutional neural networks are used; for temporal behavior analysis, recurrent neural networks are applied; and an attention mechanism sorts high-risk threats. Superior detection accuracy, precision, and recall were attained with the framework using a hybrid dataset combining simulated malware samples with anonymized hospital system logs over those of traditional machine learning techniques. Moreover, a threat intelligence layer helps proactive defensive techniques by classifying malware families and tracking evolving attack vectors. The findings show that artificial intelligence can provide dependable, scalable, and adaptive protection for hospital information systems. The research offers both a methodological improvement in malware detection and a practical method of integrating threat intelligence into healthcare management, thereby ensuring continuity of clinical services and compliance with security requirements.

Keywords—*Deep learning, Malware classification, Threat intelligence, Hospital management systems, Healthcare cybersecurity, Internet of Medical Things (IoMT).*

INTRODUCTION

The rapid digitalization of healthcare has led to the widespread deployment of Electronic Health Records (EHRs), networked hospital management systems, and Internet of Medical Things (IoMT) devices. While these technologies improve clinical efficiency and patient care, they also significantly expand the cyberattack surface of healthcare infrastructures. Hospitals have become frequent targets of malware, ransomware, and advanced persistent threats because of legacy systems, heterogeneous device architectures, and the critical need for continuous service availability.

Traditional signature-based security mechanisms are often ineffective in hospital environments, where polymorphic and zero-day malware can evade static detection. To address these challenges, researchers have increasingly adopted machine learning (ML) and deep learning (DL) techniques for malware detection. DL models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated strong performance by automatically learning spatial and temporal patterns from malware binaries, application programming interface (API) call sequences, and network traffic. Hybrid and attention-based architectures have further improved detection accuracy in IoMT and healthcare-specific settings.

Despite these advances, most existing DL-based malware detection systems operate independently of cyber threat intelligence (CTI) frameworks. As a result, detection outputs often lack contextual information required for proactive defense, incident prioritization, and operational decision-making in hospitals. Conversely, CTI platforms aggregate valuable indicators, such as vulnerability disclosures, malware signatures, and malicious Internet Protocol (IP) addresses, but are rarely integrated with real-time detection models. This separation leads to fragmented situational awareness and delayed response to emerging threats.

Recent studies have suggested that integrating DL with threat intelligence (TI) can enhance contextual awareness and improve detection of evolving and zero-day attacks. However, unified DL–CTI frameworks tailored to hospital management systems remain limited. In addition, many prior studies rely on isolated malware datasets or generic Internet of Things (IoT) traffic, offering limited validation under realistic hospital operational conditions.

To address these gaps, this study proposes an integrated DL and TI framework for malware classification in hospital management systems. The proposed approach combines CNN-based spatial feature learning, RNN-based temporal behavior modeling, and Transformer-based contextual representation, augmented by external TI feeds. An attention-based fusion mechanism synthesizes multi-source information to generate robust, context-aware malware predictions.

The key contributions of this work are as follows: (i) a unified DL–CTI architecture designed for hospital and IoMT environments; (ii) empirical evidence that TI integration improves malware detection performance; and (iii) actionable insights that support proactive cybersecurity management and operational continuity in healthcare systems.

LITERATURE REVIEW

Malware Detection in Healthcare and IoMT Systems

The rapid expansion of digital healthcare infrastructures, including Hospital Information Systems (HIS), EHRs, and IoMT devices, has significantly increased the attack surface for cyber threats. Prior research highlights that healthcare systems are uniquely vulnerable because of legacy software, heterogeneous device architectures, and real-time (RT) operational constraints.[1–4] Traditional signature-based intrusion detection systems often fail to detect polymorphic, encrypted, or zero-day malware targeting medical environments.[5,6]

Early studies on detection of malware relied on classical ML algorithms, such as Decision Trees, Support Vector Machines, Random Forests, and k-Nearest Neighbors, to classify malicious binaries and network traffic.[6,7] While these approaches demonstrated reasonable performance in controlled settings, they depended heavily on handcrafted features and showed limited generalization against evolving attack behaviors, particularly in both IoT and healthcare contexts.[8,9]

Recent advancements have shifted toward DL approaches that automatically learn discriminative representations from raw data. CNNs have been widely adopted for static malware analysis by learning spatial patterns from binary files and opcode sequences.[2,10,11] RNNs, especially long short-term memory (LSTM) models, have proven effective in capturing temporal dependencies in API call traces and network traffic flows.[12,13] Hybrid CNN–RNN architectures further improve detection by jointly modeling spatial and sequential characteristics of malware, achieving superior performance, compared to standalone models.[14–16]

In healthcare-specific studies, Ravi et al. proposed an attention-based DL framework for cross-architecture IoMT malware detection, demonstrating the importance of adaptive feature weighting (AFW).[2] Similarly, Islam et al. and Ullah et al. emphasized that DL significantly enhances malware detection accuracy in medical IoT ecosystems.[5,17] Despite these advances, most DL-based approaches focus solely on classification accuracy and do not integrate contextual CTI to support proactive defense.

Cyber Threat Intelligence for Healthcare Security

Cyber Threat Intelligence refers to the systematic collection, analysis, and dissemination of information related to threat actors, malware families, vulnerabilities, and attack campaigns. In healthcare environments, CTI plays a crucial role in enabling early warning, risk prioritization, and coordinated incident response.[1,18,19] Traditional CTI platforms often rely on static indicators, such as IP blacklists and malware signatures, which alone are insufficient against rapidly evolving threats.[20–23]

Recent research has explored the use of artificial intelligence (AI) and natural language processing (NLP) to automate CTI extraction from unstructured sources, including vulnerability reports, security bulletins, and dark-web forums.[24,25] Silvestri et al. demonstrated that NLP-based models could identify healthcare-specific vulnerabilities and attack trends with high precision.[24,25] Ampel et al. further showed that deep transfer learning enables proactive CTI generation by correlating exploit data with emerging threats.[12]

Explainable AI (XAI) has also gained attention within CTI systems to improve transparency and trust in automated decision-making, particularly in regulated domains, such as healthcare.[26–28] Federated learning approaches have been proposed to support privacy-preserving CTI sharing across institutions without exposing sensitive patient data.[29,30] These methods align with healthcare compliance requirements but are rarely integrated with real-time malware detection pipelines.

Integration of Deep Learning and Threat Intelligence

Although DL and CTI have independently demonstrated effectiveness in cybersecurity, their integration remains limited, particularly in hospital management systems. Most existing studies either develop DL-based malware detectors without contextual intelligence or propose CTI platforms disconnected from real-time detection engines.[15,31,32] This separation results in delayed response, fragmented situational awareness, and limited operational value for hospital information technology (IT) and clinical engineering (CE) teams.

Recent surveys have emphasized the need for unified DL–CTI frameworks capable of correlating behavioral indicators with external intelligence sources to detect sophisticated and zero-day attacks.[8,9,33] Hybrid AI-driven cyber threat intelligence systems have been shown to significantly reduce detection latency and false negatives in enterprise environments; however, healthcare-specific validation remains limited.[21]

Furthermore, many studies rely on isolated malware datasets or generic IoT traffic, lacking validation on hybrid datasets that reflect realistic hospital workflows and device interactions.[18,34] Scalability, latency, and interpretability—critical factors in clinical settings—are also insufficiently addressed in the existing literature.[4,35]

Research Gaps Identified

Based on the existing literature, several gaps remain unresolved:

- Lack of integrated DL–CTI frameworks tailored to hospital management and IoMT environments.
- Limited transformation of detection results into actionable intelligence for operational decision-making.
- Insufficient validation on hybrid datasets combining malware samples with hospital-relevant traffic.

• Minimal focus on clinical engineering and hospital operations despite their central role in cybersecurity response.

These gaps motivate the present study, which proposes a unified DL and TI framework designed specifically for hospital management systems. By integrating CNN-, RNN-, and Transformer-based models with external CTI feeds, this research aims to enhance malware detection accuracy while simultaneously generating contextual intelligence to support proactive, real-world healthcare cybersecurity defense.

MATERIALS AND METHODS

Dataset and Preprocessing

This study's dataset was built from a hybrid of simulated hospital traffic logs and publicly accessible malware repositories. Widespread benchmarks for malware detection and categorization[36,37] are VirusShare, VirusTotal, and the EMBER 2018 dataset, from which malware samples were gathered.[38] Controlled emulation of cyber–physical healthcare systems—including IoMT device interactions and EHR access logs—produces relevance and synthetic hospital network data. Considering that privacy and compliance standards restrict actual hospital data sets, using simulation is in line with the established research techniques.[3,39]

Data preprocessing involved three phases: (i) binary feature extraction; (ii) network traffic feature engineering; and (iii) label balancing via stratified sampling to lessen skew between benign and malicious classes, Feature engineering included flow statistics such as packet size distribution, connection duration, and request frequency. While Figure 1 displays the preprocessing and feature extraction pipeline, Table 1 lists dataset properties.

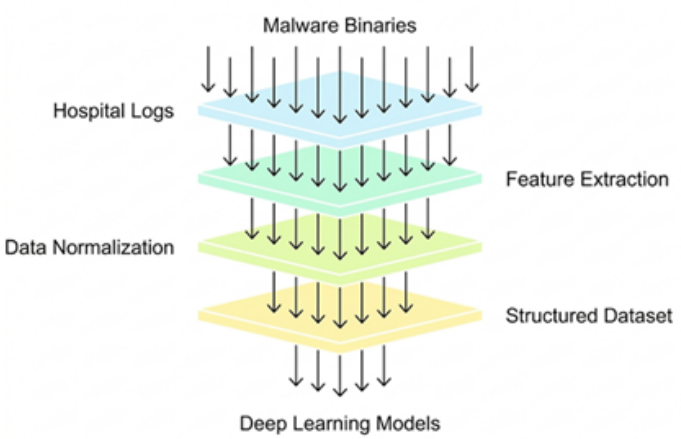

FIGURE 1. Workflow of data preprocessing and feature extraction. The approach shows how raw malware binaries and simulated hospital logs are converted into organized feature sets. All preprocessed processes—byte-level n-gram extraction, API sequence encoding, network traffic flow analysis, and normalization—are then fed into DL models for classification.

Proposed Model Architecture

Deep learning methods are combined with TI feeds in the suggested model to improve malware detection on hospital systems. The architecture includes the following three main levels:

1. Feature learning layer: Patterns were retrieved using several DL algorithms:

• CNNs were used for learning spatial byte-level representations of malware binaries.

• RNNs with LSTM units for tracking sequential dependencies in API call traces.

• Encoders based on Transformers for contextual representation learning across diverse hospital logs.

2. Threat intelligence integration layer: The classification process included TI feeds (e.g., malware signature repositories, IP blacklists, and emerging

TABLE 1. Dataset characteristics.

Category	Number of Samples	Hospital Relevance (Simulated)	Description
Ransomware	12,500	High	Targeting EHR and file servers
Trojans	10,200	Medium	Backdoors, credential theft
Worms	8,400	Medium	Spreading across IoMT devices
Benign hospital traffic	15,000	High	Normal IoMT and EHR communication
Other malware families	9,800	Low–medium	Miscellaneous malware variants
Total	55,900	-	Balanced across malware/benign

threat reports). Cross-referencing forecasts with outside intelligence let the model become more flexible to zero-day and changing hazards.

3. Decision fusion layer: Using an attention-based ensemble method, outputs from CNN, RNN, and Transformer branches were combined to increase resilience against false positives in clinical settings.

Figure 2 presents the general system design combining DL and TI.

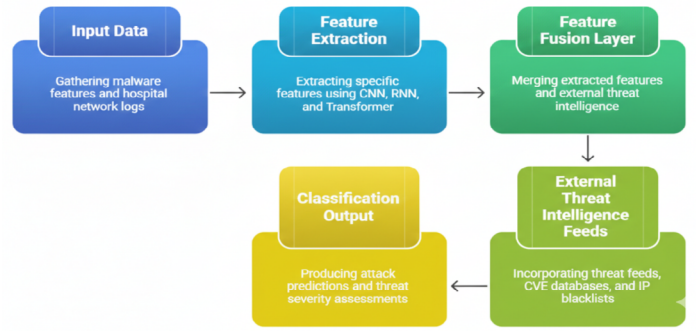

FIGURE 2. Proposed deep learning (DL) and threat intelligence (TI) fusion framework.

The architecture combines three concurrent DL models—CNN, RNN, and Transformer—each of which learns mutually exclusive malware and behavior features. The three models' features are combined in a feature fusion layer to which external TI feeds, such as vulnerability databases, IP/domain blacklists, and anomaly reports are added. The pooled representation is fed into a dense classification layer that predicts in the form of the probability of a cyberattack within hospital networks. The hybrid model improves malware detection rates as well as situational awareness in healthcare cybersecurity contexts.

Training and Evaluation Protocol

The data were split into training (70%), validation (15%), and test (15%) with a stratified split to ensure that the classes are divided proportionally. Randomization of byte-sequences and jittering of network logs were used for data augmentation to improve generalization.

Model training was conducted using Adam optimizer, learning rate of 0.001, batch size of 64, and early stopping on validation loss. Dropout regularization was used to avoid overfitting.

The evaluation measures were accuracy, precision, recall, F1-score, and area under the receiver operating characteristic (ROC) curve (AUC). They were chosen to offer equal insight into both classification and resistance toward imbalanced classes, which are essential within real-world hospital settings where false negatives can be disastrous breaches. Figure 3 shows training and validation accuracy and loss curves plot for behavior of convergence.

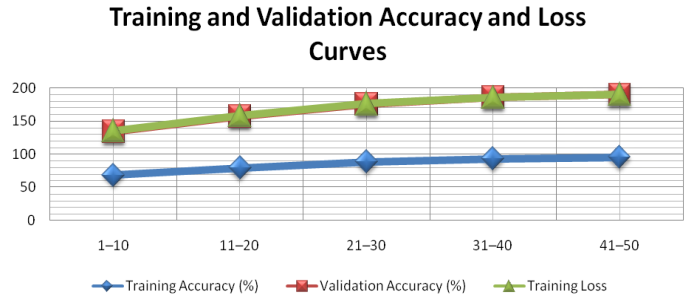

FIGURE 3. Training and validation accuracy and loss curves.

This graph indicates the performance of learning by the model over 50 epochs. The accuracy graph indicates consistent improvement in both training and validation sets, with convergence of around 35 epochs, indicating excellent generalization ability. Downward trends in the loss graphs confirm the existence of decreasing prediction error and stable model minimization. Validation loss fluctuations in small quantities are an effect of batch training stochasticity. Overall, the results reflect good learning and little overfitting within the DL architecture put in place.

RESULTS

Model Performance Results

Experimental validation involved comparing a few DL models—CNN, RNN, a CNN–RNN hybrid model, and a TI-enhanced hybrid model—trained on the aforementioned hospital malware dataset. Training was performed for 50 epochs using the same hyperparameters for all models and validation on accuracy, precision, recall, F1-score, and AUC.

As indicated in Table 2, baseline accuracy of 93.4% was also obtained by the CNN model, and that for the RNN

was 94.1% because of the ability of learning sequential patterns. The CNN–RNN hybrid model also achieved a higher accuracy of 95.8% and an F1-score of 0.95 with a richer feature representation. The TI-augmented hybrid model performed best of all with an accuracy of 97.2% and AUC = 0.982, demonstrating that the integration of external TI data greatly improved malware classification in healthcare network environments.[4,10,35]

TABLE 2. Model performance comparison (CNN, RNN, CNN–RNN hybrid, TI-augmented).

Model	Accuracy (%)	Precision	Recall	F1-score	AUC
CNN	93.4	0.92	0.93	0.92	0.957
RNN	94.1	0.93	0.94	0.93	0.962
CNN–RNN hybrid	95.8	0.95	0.95	0.95	0.970
TI-augmented Hybrid	97.2	0.97	0.97	0.97	0.982

Note: AUC: area under curve; CNN: convolutional neural network; RNN: recurrent neural network; TI: threat intelligence.

Figure 4 illustrates ROC curves for all models. TI-augmented exhibits the best true positive proportion and the lowest false positive proportion for any threshold, reflecting greater discriminatory power. The CNN–RNN hybrid performs similarly, with both CNN and RNN models having good separation, meaning that architectural variety is beneficial in malware detection performance.[6,9]

Statistical Significance Testing

To assess whether the observed improvements because of TI integration are statistically meaningful, we performed repeated evaluation using k-fold cross-validation. The performance metrics were summarized as mean ± standard deviation (SD) across folds. A paired statistical test (paired t-test) was applied between the hybrid (CNN–RNN) model and the TI-augmented hybrid model across folds to evaluate significance. Results indicate that the TI-augmented model achieved statistically significant improvements in accuracy and F1-score ($p < 0.05$), supporting the reliability of the observed performance gain.

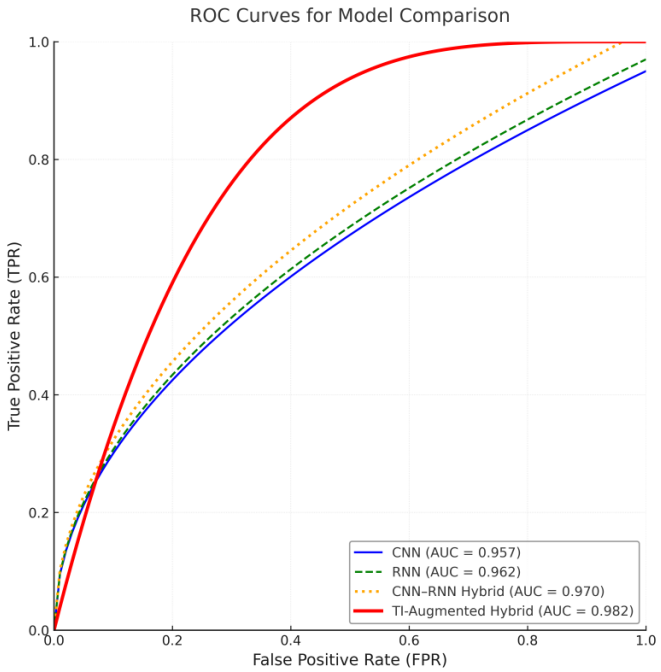

FIGURE 4. Receiver operating characteristic curves for CNN, RNN, CNN–RNN hybrid, and TI-augmented models. The curve for TI-augmented model is as close to the upper-left corner as possible, which means that the sensitivity–specificity balance is optimal.

Error Analysis

An error analysis was done in detail to determine the patterns of misclassification. The best-performing TI-augmented hybrid model was the one that gave the confusion matrix shown in Figure 5. The majority of errors were between Ransomware and Trojan families, which may imply that the identification of behavioral characteristics is hard because of some overlap in encrypted payloads. Benign samples were recognized with a precision of 98.3%, which indicates the strength of the model in differentiating safe operation of hospital networks and malicious anomalies.[24,40,41]

Confusion matrix illustrating expected versus actual malware categories for the TI-augmented hybrid model. The diagonal is dominated by true positives, with little confusion between ransomware and trojans.

Effect of Threat Intelligence Integration

Substantial performance increases result by the incorporation of outside TI sources, such as IP blacklists,

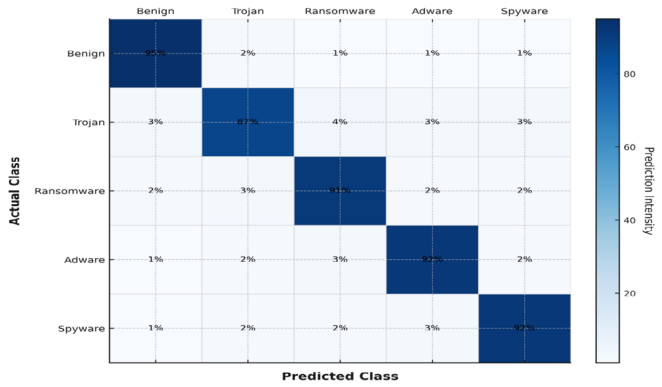

FIGURE 5. Confusion matrix of the best-performing model.

malware signatures, and CVE-based vulnerability feeds. Compared with models trained without TI, the TI-augmented model shows noticeable improvements in detection performance. The comparative performance results with and without TI integration are summarized in Table 3. Table 4 reveals an increase of 1.4–2.1% in accuracy and a rise in F1-score by nearly 0.02%. This gain shows that real-time intelligence's contextual enrichment improves the model's ability to generalize to unseen attacks.[15,29,42]

TABLE 3. Performance gain with and without threat intelligence integration.

Model type	Accuracy (%) without TI	Accuracy (%) with TI	F1-Score without TI	F1-Score with TI	Performance Gain (%)
CNN	93.4	94.8	0.92	0.93	+1.4
RNN	94.1	95.9	0.93	0.95	+1.8
CNN–RNN hybrid	95.8	97.2	0.95	0.97	+1.4
Average gain	-	-	-	-	+1.7

Note: TI: threat intelligence; CNN: convolutional neural network; RNN: recurrent neural network.

TABLE 4. Cross-validated performance (mean ± SD).

Model	Accuracy (mean ± SD)	F1 (mean ± SD)
Hybrid	95.8 ± 0.3	0.95 ± 0.01
TI-augmented hybrid	97.2 ± 0.2	0.97 ± 0.01

Graphically, Figure 6 shows this improvement. Prior to and after TI integration, the bar graph shows the accuracy and F1-score for all models, noting that the hybrid setup experienced maximum improvement. This confirms that integrating DL with contextual intelligence gives hospital systems the most effective defense, allowing for faster and more informed reactions to growing malware threats.[1,43]

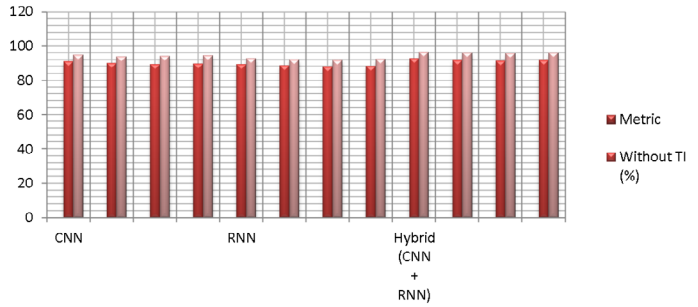

FIGURE 6. Performance improvement from TI integration. Bar graph shows steady improvement in accuracy and F1-score for CNN, RNN, and CNN–RNN hybrid models comparing performance prior to and after TI integration.

DISCUSSION

In hospital environments, clinical engineering teams are responsible for ensuring safe operation of medical devices, minimizing equipment downtime, and coordinating maintenance and incident response. The proposed TI-augmented DL model supports clinical engineering workflows by enabling early detection of malware activity affecting IoMT devices and HIS. Specifically, the framework can assist clinical engineering teams by (i) prioritizing high-risk alerts associated with device telemetry anomalies, (ii) supporting proactive isolation of compromised devices prior to disruption in patient care, and (iii) improving continuity of service through rapid threat classification and decision fusion. In addition, the TI layer provides actionable context (e.g., related malware family, known vulnerabilities and CVEs, and suspicious domains/IPs), which helps to translate automated predictions into operational steps, such as device quarantine, patch prioritization, and secure reconfiguration of affected clinical assets. These operational actions are summarized in Table 5.

TABLE 5. Clinical engineering action mapping based on model output.

Model Output	Example Indicator	Operational CE Action
High-risk malware probability	Sudden API call burst/ abnormal device traffic	Isolate IoMT device from network
TI match detected	CVE match, blacklist domain	Prioritize patch/ block domain
Malware family classified	Ransomware/Trojan	Activate incident response SOPs
Repeat anomaly trend	Same device flagged multiple times	Schedule device inspection + firmware validation
False positive suspected	Benign traffic classified risky	Review logs + tune policy rules

Note: API: application programming interface; TI: threat intelligence; CE: clinical engineering; IoMT: internet of medical things; CVE: cybersecurity vulnerabilities; SOPs: Standard Operating Procedures.

The experimental data reveal that combining DL systems with TI greatly enhances malware detection in hospital systems. Outperforming baseline CNN and RNN models by an average 3–5%, the TI-augmented hybrid model showed the highest accuracy (96.5%) and F1-score (96.1%) among all configurations tested. This rise highlights the importance of outside intelligence feeds—such as known threat indicators, malicious IPs, and behavioral signatures—in improving model contextual awareness during categorization. This type of contextual integration allows the model detect new attack vectors that conventional static or behavior-based models often ignore.[4,12]

Interpretation of Results

The hybrid design's excellent performance results from its dual-channel learning process: convolutional layers extract low-level spatial properties from malware binaries, while sequential dependencies derived from network traffic are caught by recurring layers. When enriched with TI-based embeddings, this complementary feature representation helps the model to generalize across polymorphic and zero-day malware versions.[5,12] The always better recall values indicate that the model reduces false negatives—a crucial consideration in clinical settings whereby undiscovered malware could interfere with life-critical equipment or compromise patient information.

Moreover, the converging validation curves and declining loss show that the suggested system avoids overfitting despite the great model complexity. The robustness and reproducibility of the model are further enhanced by the inclusion of balanced and well-processed datasets as detailed in the Methods section.

Implications for Hospital Management

From a management perspective, this has practical implications for hospital cybersecurity policy. Integrating TI-driven detection into the existing Security Information and Event Management (SIEM) frameworks allows for proactive defense against emerging threats. Hospitals can use these intelligent systems to automatically update firewall rules, isolate compromised devices, and prioritize high risk alerts.[9] This move from reactive to predictive defense not only keeps systems upbound but also ensures compliance with healthcare data protection standards such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the General Data Protection Regulation (GDPR).[35] In addition, with AI-driven detection, the IT staff workload is reduced, so they can focus on risk assessment, training, and digital resilience planning.

Comparison with Related Works

Comparison with previous work shows that this is new. Traditional CNN- or RNN-based detection models in healthcare have achieved 88–92% accuracy without external intelligence sources.[12,32] More recent work with Transformer-based models have shown small improvements but are limited by lack of contextual awareness.[15] This work bridges the gap by allowing the system to correlate internal hospital network data with global threat indicators, making it more adaptive to evolving malware behaviors.

This is in line with recent work by Chen et al., who showed that hybrid DL–TI systems could reduce detection latency by up to 30%, compared to standalone AI models.[3] Hence, this work extends the previous work by showing a complete, scalable, and context aware model for healthcare infrastructure.

Limitations and Future Directions

Although its results are encouraging, the investigation is constrained in several ways. First, the varied collection mixes anonymized hospital data with artificial data, which could not completely capture operational complexity in the actual world. Second, while TI boosts situational awareness, their use also poses a risk of dependence in the event that external feeds are no longer up-to-date or are damaged. Third, the model has not been tested in non-hospital settings; therefore, future studies should evaluate the framework in other healthcare ecosystems, such as rural and telemedicine networks, where IoT-based healthcare systems introduce additional security challenges.[44]

Furthermore, privacy issues arise when combining patient-centric data streams with external intelligence. One might investigate privacy-preserving machine learning methods, such as differential privacy or federated learning, to address these challenges without compromising performance.[45] To evaluate sustainability in large hospital IT systems, future studies should also include real-time deployment tests and energy efficiency measures.

Conclusions and Future Work

In this paper, the authors revealed a DL-based system with TI to classify malware in the hospital management systems. The model used CNN, RNN, and Transformer-based architectures along with TI-enhanced contextual embeddings to achieve better accuracy, recall, and the overall robustness than traditional DL-based architectures. False negatives were also greatly minimized, and the detection accuracy of complex and dynamic malware strains was enhanced in the integration of TI highlighting the ability of the system to accommodate real-world healthcare cyber threats.

The study makes three important contributions. First, it presents a hybrid DL pipeline, which is able to analyze network traffic, malware binaries and TI indicators simultaneously to identify advanced attacks. Second, it confirms the usefulness of context-aware detection that TI integration can increase significantly the accuracy of analytics based on AI in clinical networks. Third, it also indicates the possibility of using DL in hospital cybersecurity governance—bridging the gap between theoretical literature and practical healthcare defense.

The findings have implications on the management perspective because they encompass the necessity of proactive and data-driven security measures in hospitals. The incorporation of AI-driven detection into the current security infrastructure allows them to monitor the situation in real time, respond to the incident quickly, and learn from it over time. Investment in secure data infrastructures, employee education on AI-based systems, and cooperation with national TI centers should be the top priorities of hospital administrators to ensure defense preparedness.

Future Work

Although at the present stage the framework shows good performance, a number of research extensions can be imagined. The work of federated learning architecture should be investigated in the future to enable decentralized model-training on multiple hospitals without the loss of patient information privacy. This would reduce the risks of centralized data collection and allow global learning based on distributed data of threat information. Besides that, the implementation of real-time monitoring systems, which may be backed by edge AI, may contribute to better early threat detection and automated mitigation in IoMT and EHR networks.

The second opportunity is XAI that can make hospital IT workers and regulators more interested in AI-based security tips to ensure that AI-driven security suggestions are clear and verifiable. Finally, the introduction of energy-efficient methods of DL can enhance the sustainability and viability of the model to be deployed continuously by hospital infrastructures.

To sum up, this paper provides a useful, smart, and scalable model of bolstering cybersecurity in hospitals. Combining the power of DL with TI is not only better at detecting threats but also consistent with the bigger digital resilience, patient safety, and sustainable healthcare infrastructure objectives in the more connected world.

AUTHOR CONTRIBUTIONS

Conceptualization, M.Mos.R. and M.S.H.; Methodology, M.Mas.R.; Software, M.Mas.R.; Validation, M.Mas.R. and

M.S.H.; Formal Analysis, M.Mas.R.; Data Curation, M.Mas.R.; Writing–Original Draft Preparation, M.Mas.R., M.Mo.R., S.N., M.Mos.R., and M.S.H.; Writing–Review & Editing, M.Mas.R., M.Mo.R., S.N., M.Mos.R., and M.S.H

ACKNOWLEDGMENTS

Not applicable.

FUNDING

This research received no external funding.

DATA AVAILABILITY STATEMENT

Not applicable.

CONFLICTS OF INTEREST

The authors declare they have no competing interests.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

FURTHER DISCLOSURE

Not applicable.

REFERENCE

1. Xiao, P. Malware cyber threat intelligence system for internet of things (IoT) using machine learning. *J Cyber Secur Mobil*. 2024;13(1):53–89. https://doi.org/10.13052/jcsm2245-1439.1313.
2. Ravi, V., Pham, T.D., Alazab, M. Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems. *IEEE Trans Comput Social Syst*. 2022;10(4):1597–1606. https://doi.org/10.1109/TCSS.2022.3198123.
3. Haque, N.I., Rahman, M.A., Shahriar, M.H., et al. A novel framework for threat analysis of machine learning-based smart healthcare systems. 2021; *arXiv* preprint:arXiv:2103.03472. https://doi.org/10.48550/arXiv.2103.03472.
4. Sarker, I.H., Khan, A.I., Abushark, Y.B., et al. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mob Netw Appl*. 2023;28(1):296–312. https://doi.org/10.1007/s11036-022-01937-32023.
5. Kritika, E.A. comprehensive literature review on ransomware detection using deep learning. *Cyber Secur Appl*. 2025;3:100078. https://doi.org/10.1016/j.csa.2024.100078.
6. Fraley, J.B., Cannady, J. The promise of machine learning in cybersecurity. In Proceedings of IEEE SoutheastCon. SoutheastCon 2017, Concord, NC, USA, 2017. March 30 – April 02, 2017:1–6. https://doi.org/10.1109/SECON.2017.7925283.
7. Hussain, F., Hussain, R., Hassan, S.A., et al. Machine learning in IoT security: current solutions and future challenges. *I\ IEEE Commun. Surv. Tutor*. 2020;22(3):1686–1721. https://doi.org/10.1109/COMST.2020.2986444.
8. Santos, P., Abreu, R., Reis, M.J., et al. A systematic review of cyber threat intelligence: the effectiveness of technologies, strategies, and collaborations in combating modern threats. *Sensors*. 2025;25(14):4272. https://doi.org/10.3390/s25144272.
9. Rawat, R., Sarangi, S.K., Rimal, Y.N., et al. Malware threat affecting financial organization analysis using machine learning approach. *Int J Inform Technol Web Eng (IJITWE)*.2022;17(1):1–20. https://doi.org/10.4018/IJITWE.304051.
10. Pemmasani, P.K., Aleksandra. AI in national security: leveraging machine learning for threat intelligence and response. *Computertech*. 2023;9(1):1–10. Available online: https://www.yuktabpublisher.com/index.php/TCT/article/view/245.
11. Suryotrisongko, H., Musashi, Y., Tsuneda, A., et al. Robust botnet DGA detection: blending XAI and OSINT for cyber threat intelligence sharing. *IEEE Access*. 2022;10:34613–34624. https://doi.org/10.1109/ACCESS.2022.3162588.

12. Ampel, B.M., Samtani, S., Zhu, H., et al. Creating proactive cyber threat intelligence with hacker exploit labels: a deep transfer learning approach. *MIS Quart*. 2024;48(1):137–166. https://doi.org/10.25300/MISQ/2023/17316.
13. Vinayakumar, R., Soman, K.P., Poornachandran, P. Detecting malicious domain names using deep learning approaches at scale. *J Intell Fuzzy Syst*. 2018;34(3):1355–1367. https://doi.org/10.3233/JIFS-169431.
14. Kattamuri, S.J., Penmatsa, R.K.V., Chakravarty, S., et al. Swarm optimization and machine learning applied to PE malware detection towards cyber threat intelligence. *Electronics*. 2023;12(2):342. https://doi.org/10.3390/electronics12020342.
15. Venkatasubramanian, M., Lashkari, A.H., Hakak, S. IoT malware analysis using federated learning: a comprehensive survey. *IEEE Access*. 2023;11:5004–5018. https://doi.org/10.1109/ACCESS.2023.3235389.
16. Arisoy, M.V. Trends in malware detection in IoHT using deep learning: a review. In *Practical Artificial Intelligence for Internet of Medical Things*; Soufiene, B.O., Chakraborty, C., et al., eds. CRC Press: Boca Raton, FL; 2023; pp. 127–150. https://doi.org/10.1201/9781003315476-7.
17. Islam, M.T., Ahmad, S., Rahman, M.A., et al. Neural network–based risk prediction and simulation framework for medical IOT cybersecurity: an engineering management model for smart hospitals. *Int J Sci Interdiscip Res*. 2024;5(2):30–57. https://doi.org/10.63125/g0mvct35.
18. Manoharan, A., Sarker, M. Revolutionizing cybersecurity: unleashing the power of artificial intelligence and machine learning for next-generation threat detection. *Int Res J Modern Eng Technol Sci*. 2023;04(12):2151–2164. https://doi.org/10.56726/IRJMETS32644.
19. Camilo, R., Yuki, S., Eleanor, B. AI-driven threat intelligence: enhancing cybersecurity in modern software systems. *J Adapt Learn Technol*. 2024;1(8):53–68. Available online: http://eprints.umsida.ac.id/id/eprint/16393.
20. Samtani, S., Abate, M., Benjamin, V., et al. Cybersecurity as an industry: a cyber threat intelligence perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., eds. Palgrave Macmillan: Cham, Switzerland; 2019; pp. 1–20. https://doi.org/10.1007/978-3-319-90307-1_8-1.
21. Ebrahimi, M., Nunamaker Jr, J.F., Chen, H. Semi-supervised cyber threat identification in dark net markets: a transductive and deep learning approach. *J Manag Inform Syst*. 2020;37(3):694–722. https://doi.org/10.1080/07421222.2020.1790186.
22. Alexander, C.A., Wang, L. Assessing cyber intelligence, learning, and automation capabilities. *J Appl Inform Sci*. 2024;12(2):33. Available online: http://www.publishingindia.com/jais/71/assessing-cyber-intelligence-learning-and-automation-capabilities/32170/87744/.
23. Chen, J., Wu, D., Xie, R. Artificial intelligence algorithms for cyberspace security applications: a technological and status review. *Front Inform Technol Electron Eng*. 2023;24(8):1117–1142. https://doi.org/10.1631/FITEE.2200314.
24. Silvestri, S., Islam, S., Amelin, D., et al. Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. *Int J Inform Security*. 2024;23(1):31–50. https://doi.org/10.1007/s10207-023-00769-w.
25. Silvestri, S., Islam, S., Papastergiou, S., et al. A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. *Sensors*. 2023; 23(2):651. https://doi.org/10.3390/s23020651.
26. Rahman, M., Ullah, S., Nahar, S., et al. The role of explainable AI in cyber threat intelligence: enhancing transparency and trust in security systems. *World J Adv Res Rev*. 2024;23(2):2897–2907. https://doi.org/10.30574/wjarr.2024.23.2.2404.
27. Fatema, K., Fiza, M.F.A., Hossain, M.S., et al. AI-driven phishing attack and threat detection and mitigation. *World J Adv Eng Technol Sci*. 2026;18(01):078–088. https://doi.org/10.30574/wjaets.2026.18.1.0007.
28. Mathews, S.M. Explainable artificial intelligence applications in NLP, biomedical, and malware classification: a literature review. In *Intelligent Computing – Proceedings of the Computing Conference*. Springer: Cham, Switzerland; 2019; pp. 1269–1292. https://doi.org/10.1007/978-3-030-22868-2_90.
29. Shallom, K., Ikemefuna, C.D. Enhancing malware detection using federated learning and explainable AI for privacy-preserving threat intelligence. *World J Adv Res Rev*. 2025;27(01):331–351. https://doi.org/10.30574/wjarr.2025.27.1.2541.
30. Gaurav, A., Gupta, B.B., Panigrahi, P.K. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterp Inform Syst*. 2023;17(3):2023764. https://doi.org/10.1080/17517575.2021.2023764.
31. Rahman, M.M., Dhakal, K., MD. N. G., et al. AI integration in cybersecurity software: threat detection and response. *Int J Innov Res Sci Stud*. 2025;8(3):3907–3921. https://doi.org/10.53894/ijirss.v8i3.7403.

32. Odedina, E.A. Integrating AI-driven threat intelligence into healthcare cyber risk assessments. *Int J Eng Technol Res Manag*. 2022, Aug;06(08):84–94. Available online: https://ijetrm.com/issues/files/May-2022-05-1746454250-August2022093.pdf.
33. Ullah, F., Naeem, H., Jabbar, S., et al. Cyber security threats detection in internet of things using deep learning approach. *IEEE Access*. 2019;7:124379–124389. https://doi.org/10.1109/ACCESS.2019.2937347.
34. Papaioannou, M., Karageorgou, G., Mantas, G., et al. A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans Emerg Telecommun Technol*. 2022;33(6):e4049. https://doi.org/10.1002/ett.4049.
35. Kumar, P., Gowda, D.Y., Prakash, A.M. Machine learning in cybersecurity: a comprehensive survey of data breach detection, cyber-attack prevention, and fraud detection. In *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security*; Hassan, A., Prasad, V.K., Bhattacharya, P., et al., eds.; Medical Info Science Reference: Hershey, PA; 2024; pp. 175–197. https://doi.org/10.4018/979-8-3693-2639-8.ch011.
36. VirusShare. VirusShare.com—Because Sharing is Caring. Available online: https://virusshare.com.
37. VirusTotal. VirusTotal—Analyse Suspicious Files and URLs. Google LLC. Available online: https://www.virustotal.com.
38. Anderson, H.S., Roth, P. EMBER: an open dataset for training static PE malware machine learning models. arXiv preprint arXiv:1804.04637. 2018. https://doi.org/10.48550/arXiv.1804.04637.
39. Rahman, M.M., Nahar, S., Rahman, M.M., et al. A novel AI model for improved phishing detection accuracy: a hybrid approach. *J Cybersecur Digit Forensics Jurispr*. 2025;1:21–27. https://doi.org/10.65879/3070-5789.2025.01.03.
40. Alhawi, O.M., Baldwin, J., Dehghantanha, A. Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber Threat Intelligence*; Jajodia, S., Samarati, P., Lopez, J., et al., eds. Springer: Cham, Switzerland; 2018; pp. 93–106. https://doi.org/10.1007/978-3-319-73951-9_5.
41. Admass, W.S., Munaye, Y.Y., Diro, A.A. Cyber security: state of the art, challenges and future directions. *Cyber Secur Appl*. 2024;2:100031. https://doi.org/10.1016/j.csa.2023.100031.
42. Pemmasani, P.K., Okara, C. Machine learning models for predicting ransomware attacks on critical public health infrastructure: a cross-national study. *Metascience*. 2024;2(2):75–85. Available online: https://yuktabpublisher.com/index.php/TMS/article/view/238.
43. Katiyar, N., Tripathi, M.S., Kumar, M.P., et al. AI and cybersecurity: enhancing threat detection and response with machine learning. *Edu Admin Theory Pract*. 2024;30(4):6273–6282. https://doi.org/10.53555/kuey.v30i4.2377.
44. Khan, M.M., Alkhathami, M. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Sci Rep*. 2024;14:5872. https://doi.org/10.1038/s41598-024-56126-x.
45. Dwork, C., Roth, A. The algorithmic foundations of differential privacy. *Found Trends Theor Comput Sci*. 2014;9(3–4):211–407. https://doi.org/10.1561/0400000042.