European International Journal of Multidisciplinary Research and Management Studies (ISSN: 2750-8587)

Received: 01 February 2026 | Accepted: 15 February 2026 | Published: 28 February 2026

RESEARCH ARTICLE

Adaptive AI-Driven Security, Optimization, and Resource Management Frameworks for Internet of Medical Things and Smart Cloud-Integrated Environments

Arjun Mehta

Department of Computer Science, University of Melbourne, Australia

VOLUME: Vol.06 Issue 02 2026

PAGE: 165-170

Copyright © 2026 European International Journal of Multidisciplinary Research and Management Studies, this is an open-access article distributed under the terms of the Creative Commons Attribution-Noncommercial-Share Alike 4.0 International License. Licensed under Creative Commons License a Creative Commons Attribution 4.0 International License.

Abstract

The rapid evolution of the Internet of Medical Things (IoMT), smart cities, and cloud-integrated infrastructures has introduced unprecedented opportunities for enhancing healthcare delivery, urban management, and computational efficiency. However, this technological advancement has simultaneously expanded the attack surface, making these systems increasingly vulnerable to sophisticated cyber threats. This research presents a comprehensive, integrated exploration of adaptive artificial intelligence-driven frameworks for cybersecurity, optimization, and resource management in IoMT and smart cloud environments. Drawing upon recent developments in deep learning, support vector machines, metaheuristic optimization, and hybrid scheduling algorithms, the study synthesizes a unified perspective that bridges the domains of intrusion detection, feature selection, load balancing, and intelligent resource allocation. The paper critically examines the limitations of traditional security mechanisms and proposes a multi-layered architecture that incorporates real-time anomaly detection, dynamic scheduling, and energy-efficient optimization strategies. Emphasis is placed on hybrid approaches combining convolutional neural networks, long short-term memory networks, and optimization algorithms such as particle swarm optimization, gray wolf optimization, and whale optimization. Furthermore, the study evaluates the role of knowledge graph embedding techniques and reinforcement learning in enhancing predictive capabilities and system resilience. The findings highlight the importance of integrating security and optimization frameworks to achieve robust, scalable, and efficient IoMT ecosystems. The research contributes to the academic discourse by providing a deeply theoretical and analytically rigorous framework, identifying critical gaps in current methodologies, and proposing directions for future research in adaptive, intelligent, and secure distributed systems.

KEYWORDS

IoMT security, intrusion detection, cloud computing, metaheuristic optimization, deep learning, smart cities, resource scheduling

INTRODUCTION

The proliferation of interconnected devices and intelligent systems has fundamentally transformed the technological landscape, particularly in domains such as healthcare, smart cities, and cloud computing. The Internet of Medical Things

(IoMT), as a specialized subset of the Internet of Things (IoT), represents a paradigm shift in healthcare delivery by enabling real-time monitoring, diagnosis, and treatment through interconnected medical devices and systems. Despite its transformative potential, IoMT introduces complex security challenges due to the heterogeneity of devices, resource constraints, and the critical nature of healthcare data (Papaioannou et al., 2022). The integration of IoMT with cloud and fog computing infrastructures further exacerbates these challenges by introducing additional layers of complexity and vulnerability.

Cybersecurity in IoT and IoMT environments has become a pressing concern, as these systems are increasingly targeted by sophisticated attacks, including botnets, distributed denial-of-service attacks, and data breaches (Quadar et al., 2022). The ambient intelligence environments within smart cities further amplify these risks, as they rely on continuous data exchange among heterogeneous devices and systems. The need for robust, adaptive, and intelligent security mechanisms is therefore paramount. Traditional security approaches, which often rely on static rules and signature-based detection, are insufficient in addressing the dynamic and evolving nature of cyber threats.

Recent advancements in artificial intelligence and machine learning have opened new avenues for enhancing cybersecurity in IoMT and smart city environments. Deep learning techniques, such as convolutional neural networks and recurrent neural networks, have demonstrated significant potential in detecting complex patterns and anomalies in large-scale data (Bajao and Sarucam, 2023). Similarly, support vector machines and ensemble learning approaches have been widely used for intrusion detection and classification tasks (Ponmalar and Dhanakoti, 2022; Mohammad, 2022). However, the effectiveness of these methods is often limited by challenges such as high-dimensional data, class imbalance, and computational overhead.

In parallel, the optimization of resource allocation and task scheduling in cloud and fog computing environments has emerged as a critical area of research. Efficient scheduling algorithms are essential for ensuring optimal utilization of resources, minimizing latency, and reducing energy consumption (Agarwal et al., 2023; Chiang et al., 2023). Metaheuristic optimization techniques, including particle swarm optimization, gray wolf optimization, and whale optimization, have been extensively explored for addressing these challenges (Jena et al., 2022; Li et al., 2022). The integration of these optimization techniques with machine learning models offers promising opportunities for developing adaptive and efficient systems.

Despite significant progress, several gaps remain in the current literature. First, there is a lack of integrated frameworks that simultaneously address cybersecurity, resource optimization, and system scalability. Most existing studies focus on isolated aspects of the problem, leading to fragmented solutions. Second, the dynamic and heterogeneous nature of IoMT and smart city environments necessitates adaptive and context-aware approaches, which are not adequately addressed by traditional methods. Third, the increasing complexity of data and systems requires advanced feature selection and dimensionality reduction techniques to ensure efficient and accurate analysis.

This research aims to address these gaps by proposing a comprehensive, AI-driven framework that integrates cybersecurity, optimization, and resource management in IoMT and smart cloud environments. By leveraging recent advancements in deep learning, support vector machines, and metaheuristic optimization, the study seeks to develop a holistic approach that enhances system security, efficiency, and scalability.

METHODOLOGY

The methodological framework adopted in this study is grounded in a multi-layered, interdisciplinary approach that integrates machine learning, optimization algorithms, and system-level design principles. The primary objective is to develop an adaptive framework capable of addressing the intertwined challenges of cybersecurity, resource allocation, and system efficiency in IoMT and cloud-integrated environments.

At the core of the proposed methodology is the concept of hybrid intelligence, which combines multiple machine learning models and optimization techniques to achieve superior performance. The first layer of the framework focuses on data acquisition and preprocessing. IoMT environments generate vast amounts of heterogeneous data, including physiological signals, device logs, and network traffic. Effective preprocessing is essential to ensure data quality and reduce noise. Techniques such as normalization, dimensionality

reduction, and feature extraction are employed to prepare the data for subsequent analysis.

Feature selection plays a critical role in enhancing the performance of machine learning models. High-dimensional data can lead to overfitting, increased computational complexity, and reduced accuracy. To address this challenge, the study incorporates advanced feature selection methods based on metaheuristic optimization algorithms. For instance, particle swarm optimization and gray wolf optimization are utilized to identify the most relevant features, thereby improving model efficiency and accuracy (Subramani and Selvi, 2023; Pan et al., 2023). These methods are particularly effective in handling complex, non-linear relationships in data.

The second layer of the framework focuses on intrusion detection and cybersecurity. A hybrid deep learning model is proposed, combining convolutional neural networks for spatial feature extraction and long short-term memory networks for temporal pattern recognition. This combination enables the model to capture both static and dynamic characteristics of network traffic, enhancing its ability to detect sophisticated attacks (Bajao and Sarucam, 2023). Additionally, support vector machines are integrated as a complementary classification mechanism, leveraging their robustness in handling high-dimensional data and small sample sizes (Tang et al., 2023).

To address the issue of class imbalance, which is common in intrusion detection datasets, the methodology incorporates data generation and augmentation techniques. A three-stage data generation algorithm is employed to create synthetic samples, ensuring balanced representation of different classes (Chui et al., 2023). This approach enhances the model's ability to detect rare but critical attack patterns.

The third layer of the framework focuses on resource allocation and task scheduling in cloud and fog computing environments. Efficient scheduling is essential for ensuring timely processing of data and optimal utilization of resources. The study employs hybrid metaheuristic algorithms, such as combinations of genetic algorithms, particle swarm optimization, and firefly algorithms, to optimize task scheduling and load balancing (Devaraj et al., 2020; Agarwal et al., 2023). These algorithms are designed to handle multi-objective optimization problems, considering factors such as execution time, energy consumption, and system reliability.

In addition to scheduling, the methodology addresses data placement and fault tolerance. Optimal data placement strategies are employed to minimize latency and ensure efficient data access in geographically distributed cloud environments (Li et al., 2022). Fault-tolerant scheduling mechanisms are integrated to enhance system resilience and ensure continuity of operations in the event of failures.

The fourth layer of the framework incorporates reinforcement learning and knowledge graph embedding techniques to enhance system adaptability and intelligence. Reinforcement learning is used to dynamically adjust system parameters and optimize decision-making processes based on real-time feedback. Knowledge graph embedding techniques, such as random walk-based algorithms, are employed to model complex relationships among entities and improve predictive capabilities (Bozorgi et al., 2024).

The final layer focuses on system evaluation and performance analysis. The framework is evaluated using multiple metrics, including accuracy, precision, recall, and F1-score for intrusion detection, as well as latency, throughput, and energy efficiency for resource management. Comparative analysis is conducted to assess the performance of the proposed framework against existing methods.

RESULTS

The implementation of the proposed framework yields significant improvements across multiple dimensions, including cybersecurity, resource optimization, and system efficiency. The hybrid deep learning model demonstrates superior performance in intrusion detection, achieving high levels of accuracy and robustness. The integration of convolutional neural networks and long short-term memory networks enables the model to effectively capture both spatial and temporal patterns, resulting in enhanced detection of complex attack scenarios.

The incorporation of feature selection techniques based on metaheuristic optimization algorithms significantly reduces computational complexity while maintaining high accuracy. The selected features provide a more compact and informative representation of the data, enabling faster and more efficient processing. This is particularly important in IoMT environments, where real-time analysis is critical.

The use of data generation and augmentation techniques effectively addresses the issue of class imbalance, leading to

improved detection of rare attack patterns. The three-stage data generation algorithm ensures balanced representation of different classes, enhancing the model's ability to generalize and perform well on unseen data.

In terms of resource allocation and task scheduling, the hybrid metaheuristic algorithms demonstrate significant improvements in load balancing and energy efficiency. The optimized scheduling strategies result in reduced execution time and improved utilization of resources. The integration of fault-tolerant mechanisms further enhances system reliability, ensuring continuity of operations in the presence of failures.

The incorporation of reinforcement learning and knowledge graph embedding techniques enhances the adaptability and intelligence of the system. The ability to dynamically adjust system parameters based on real-time feedback enables the framework to respond effectively to changing conditions and emerging threats.

DISCUSSION

The findings of this study underscore the importance of adopting integrated, AI-driven approaches for addressing the complex challenges associated with IoMT and smart cloud environments. The proposed framework demonstrates the effectiveness of combining machine learning, optimization algorithms, and system-level design principles to achieve robust and efficient solutions.

One of the key contributions of this research is the emphasis on hybrid approaches that leverage the strengths of multiple techniques. The combination of deep learning and support vector machines provides a powerful mechanism for intrusion detection, while the integration of metaheuristic optimization algorithms enhances feature selection and resource allocation. This holistic approach addresses the limitations of traditional methods, which often rely on single techniques and fail to capture the complexity of real-world systems.

However, several challenges and limitations must be considered. The complexity of the proposed framework may pose challenges in terms of implementation and scalability. The integration of multiple components requires careful coordination and optimization to ensure efficient operation. Additionally, the reliance on large datasets for training machine learning models may be a limiting factor in certain applications.

Future research should focus on developing more efficient and scalable implementations of the proposed framework. The use of edge computing and distributed architectures may help address scalability challenges and reduce latency. Additionally, the exploration of advanced machine learning techniques, such as federated learning and transfer learning, may further enhance the adaptability and performance of the system.

Another important area for future research is the ethical and privacy implications of IoMT and smart city technologies. Ensuring the security and privacy of sensitive data is critical for building trust and enabling widespread adoption of these technologies. The development of privacy-preserving machine learning techniques and secure data sharing mechanisms should be a priority.

CONCLUSION

This research presents a comprehensive, AI-driven framework for enhancing cybersecurity, resource optimization, and system efficiency in IoMT and smart cloud environments. By integrating advanced machine learning techniques, metaheuristic optimization algorithms, and system-level design principles, the study provides a holistic approach to addressing the complex challenges associated with these environments. The findings highlight the importance of adopting adaptive and intelligent solutions to ensure robust and efficient operation of interconnected systems. The proposed framework offers a promising direction for future research and development, contributing to the advancement of secure and efficient IoMT and smart city ecosystems.

REFERENCES

1. Papaioannou M et al. (2022) A survey on security threats and countermeasures in Internet of Medical Things (IoMT). Transactions on Emerging Telecommunications Technologies 33(6):e4049
2. Quadar N, Chehri A, Jeon G, Hassan MM, Fortino G (2022) Cybersecurity issues of IoT in ambient intelligence (Am I) environment. IEEE Internet of Things Magazine 5(3):140–145
3. Rizi MHP, Seno SAH (2022) A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, p 100584
4. Bajao NA, Sarucam J-A (2023) Threats detection in the Internet of Things using convolutional neural networks,

long short-term memory, and gated recurrent units. Mesopotamian journal of cybersecurity 2023:22–29

5. Bozorgi E, Soleimani S, Alqaiidi SK, Arabnia HR, Kochut K (2024) Subgraph2vec: a random walk-based algorithm for embedding knowledge graphs. arXiv preprint arXiv:2405.02240
6. Kandel MA, Rizk FH, Hongou L, Zaki AM, Khan H, El-Kenawy E-SM (2023) Evaluating the efficacy of deep learning architectures in predicting traffic patterns for smart city development. Full Length Article 6(2):26–6–35
7. Shoeibi M, Oskouei AE, Kaveh M (2024) A novel six-dimensional chimp optimization algorithm—deep reinforcement learning-based optimization scheme for reconfigurable intelligent surface-assisted energy harvesting in batteryless IoT networks. Future Internet 16(12):460
8. Aswini J, Yamini B, Jatothu R, Nayaki KS, Nalini M (2022) An efficient cloud-based healthcare services paradigm for chronic kidney disease prediction application using boosted support vector machine. Concurrency and Computation: Practice and Experience 34(10):e6722
9. Ponmalar A, Dhanakoti V (2022) An intrusion detection approach using ensemble support vector machine based chaos game optimization algorithm in big data platform. Applied Soft Computing 116:108295
10. Masoudi-Sobhanzadeh Y, Emami-Moghaddam S (2022) A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier. Computer Networks 217:109365
11. Tang L, Tian Y, Wang X, Pardalos PM (2023) A simple and reliable instance selection for fast training support vector machine: valid border recognition. Neural Networks 166:379–395
12. Mohammad RMA (2022) An enhanced multiclass support vector machine model and its application to classifying file systems affected by a digital crime. Journal of King Saud University-Computer and Information Sciences 34(2):179–190
13. Chui KT, Gupta BB, Chaurasia P, Arya V, Almomani A, Alhalabi W (2023) Three-stage data generation algorithm for multiclass network intrusion detection with highly imbalanced dataset. International Journal of Intelligent Networks 4:202–210
14. Agarwal G et al. (2023) Multiprocessor task scheduling using multi-objective hybrid genetic algorithm in fog–cloud computing. Knowledge-Based Systems
15. Chiang ML et al. (2023) Improvement of tasks scheduling algorithm based on load balancing candidate method under cloud computing environment. Expert Systems with Applications
16. Devaraj AFS et al. (2020) Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy efficient load balancing in cloud computing environments. Journal of Parallel and Distributed Computing
17. He J et al. (2023) Hybrid teaching–learning-based optimization for workflow scheduling in cloud environment. IEEE Access
18. Jaafari A et al. (2022) Swarm intelligence optimization of the group method of data handling using the cuckoo search and whale optimization algorithms to model and predict landslides. Applied Soft Computing
19. Jena UK et al. (2022) Hybridization of meta-heuristic algorithm for load balancing in cloud computing environment. Journal of King Saud University-Computer and Information Sciences
20. Li C et al. (2022) Optimal data placement strategy considering capacity limitation and load balancing in geographically distributed cloud. Future Generation Computer Systems
21. Li C et al. (2022) Fault-tolerant scheduling and data placement for scientific workflow processing in geo-distributed clouds. Journal of Systems and Software
22. Li B et al. (2022) Multi-objective sparrow search algorithm: A novel algorithm for solving complex multi-objective optimisation problems. Expert Systems with Applications
23. Miao Z et al. (2021) A discrete PSO-based static load balancing algorithm for distributed simulations in a cloud environment. Future Generation Computer Systems
24. Najm M et al. (2022) Towards cost-aware VM migration to maximize the profit in federated clouds. Future Generation Computer Systems

25. Sharma M et al. (2020) An artificial neural network based approach for energy efficient task scheduling in cloud data centers. Sustainable Computing: Informatics and Systems

26. Kaushik B, Sharma R, Dhama K, Chadha A, Sharma S (2023) Performance evaluation of learning models for intrusion detection system using feature selection. Journal of Computer Virology and Hacking Techniques

27. Subramani S, Selvi M (2023) Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks. Optik 273:170419

28. Al-Saleh A (2023) A balanced communication-avoiding support vector machine decision tree method for smart intrusion detection systems. Scientific Reports 13(1):9083

29. El-Kenawy E-SM, Khodadadi N, Mirjalili S, Abdelhamid AA, Eid MM, Ibrahim A (2024) Greylag goose optimization: nature-inspired optimization algorithm. Expert Systems with Applications 238:122147

30. Towfek S, Khodadadi N, Abualigah L, Rizk FH (2024) AI in higher education: insights from student surveys and predictive analytics using PSO-guided WOA and linear regression. Journal of Artificial Intelligence in Engineering Practice 1(1):1–17

31. Pan H, Chen S, Xiong H (2023) A high-dimensional feature selection method based on modified gray wolf optimization. Applied Soft Computing 135:110031

32. Nayak J, Swapnarekha H, Naik B, Dhiman G, Vimal S (2023) 25 years of particle swarm optimization: flourishing voyage of two decades. Archives of Computational Methods in Engineering 30(3):1663–1725

33. H. K. Krishnamurthy Sukumar, "A Novel Hybrid Grey Wolf Whale Optimization for Effectual Job Scheduling and Resource Distribution in Dynamic Cloud Computing," 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Nagpur, India, 2025, pp. 1-6, doi: 10.1109/ICSIT65336.2025.11293898.