International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms

Naveen Sai Bommina[1], Uppu Lokesh[2], Nandipati Sai Akash [3], Dr. Hussain Syed [4], Dr. Syed Umar[5]

Submitted: 02/08/2023 **Revised**: 17/09/2024 **Accepted**: 28/09/2024

Abstract: The exponential growth of Internet of Things (IoT) networks has introduced unprecedented challenges in securing heterogeneous and resource-constrained devices against evolving cyber threats. This research proposes a novel framework that integrates Artificial Intelligence (AI)-driven security protocols with metaheuristic optimization techniques to enhance the resilience and efficiency of IoT networks. The AI models, including lightweight neural networks and anomaly detection systems, are designed to identify intrusion patterns and unauthorized behavior in real time. To improve the adaptability and performance of these models, metaheuristic algorithms—such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Grey Wolf Optimizer (GWO)—are employed to optimize hyperparameters, rule sets, and decision thresholds within the security protocols. The multi-objective optimization process considers key factors such as detection accuracy, energy consumption, latency, and false positive rate. Experimental results on standard IoT benchmark datasets demonstrate that the optimized AI-security protocol framework significantly outperforms traditional approaches in both detection speed and resource efficiency. This work contributes a robust, scalable, and intelligent defense mechanism for next-generation IoT infrastructures.

Keywords: IoT Security, Artificial Intelligence, Metaheuristic Algorithms, Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Anomaly Detection, Intrusion Prevention, AI Optimization, Smart Networks, Adaptive Security, Cybersecurity in IoT, Resource-Constrained Devices, Secure Communication, Intelligent Protocols.

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern communication systems by enabling seamless interconnectivity among billions of devices, ranging from household appliances to industrial machinery and critical healthcare systems. This hyper-connectivity promises improved automation, data-driven insights, and operational efficiency. However, it also introduces significant security and privacy challenges due to the decentralized nature, limited computational power, and heterogeneity of IoT devices. Traditional security protocols, often designed for static, centralized systems, are inadequate for addressing the dynamic and distributed architecture of IoT networks.

As cyber threats become more sophisticated and frequent, ensuring the integrity, confidentiality, and availability of data within IoT environments has become a critical concern. AI-driven security protocols have emerged as a promising solution, offering the ability to learn from data, adapt to emerging threats, and respond in real-time. These protocols leverage machine learning (ML) and deep learning (DL) techniques for tasks such as anomaly detection, intrusion prevention, and threat intelligence. Despite their potential, the performance of AI models is often dependent on complex and computationally expensive training processes, particularly in resource-constrained IoT settings.

To address these limitations, metaheuristic algorithms have gained attention for their ability to efficiently solve high-dimensional optimization problems without the need for gradient information or explicit models. Algorithms such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO) provide robust solutions for optimizing AI models by tuning hyperparameters, selecting features, and improving decision logic. When integrated with AI-driven security protocols, these algorithms enhance adaptability, scalability, and efficiency across diverse IoT networks.

1. Student, Department of Computer Science and Engineering University of South Florida, Tampa, Florida
2. Student, Department of Computer Science and Engineering, Oklahoma City University, Oklahoma City, Oklahoma.
3. Student, Department of Computer Science and Engineering, Campbellsville University, Campbellsville, Kentucky
4. Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.
5. Professor, Department of Computer Science & Engineering, Marwadi University, India.
E-mail:1.,bomminanaveensai1@gmail.com,1..uppulokesh666@gmail.com2, nandipatisaiakash@gmail.com3 hussain.syed@vitap.ac.in,4.umar332@gmail.com

IoT Security

The Internet of Things (IoT) represents a transformative technology ecosystem that connects a vast array of devices—ranging from smart sensors and wearables to industrial control systems—enabling them to communicate, share data, and perform autonomous operations. Despite its benefits, IoT introduces significant security challenges due to its inherent architectural and operational characteristics.

IoT devices are often resource-constrained, with limited processing power, memory, and energy supply, making the implementation of traditional security protocols difficult. Furthermore, these devices operate in heterogeneous and dynamic environments, increasing the attack surface and vulnerability to cyber threats such as data breaches, denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, and firmware tampering.

One of the fundamental issues in IoT security is the lack of standardized security frameworks across different platforms and vendors, leading to fragmented protection mechanisms. Additionally, many IoT devices are deployed with default or hardcoded credentials, outdated firmware, and poor encryption practices, further exacerbating security risks.

To address these challenges, security in IoT must encompass several layers, including:

- Authentication and Authorization – Ensuring that only trusted devices and users have access to the network and its services.
- Data Confidentiality and Integrity – Protecting data from unauthorized access or tampering during transmission and storage.
- Secure Communication Protocols – Implementing lightweight, encrypted protocols suited for constrained devices (e.g., DTLS, CoAP, MQTT with TLS).
- Real-Time Threat Detection – Utilizing machine learning and anomaly detection systems to identify and mitigate threats dynamically.
- Firmware and Software Updates – Supporting secure, over-the-air updates to patch vulnerabilities without disrupting device operation.

AI-driven approaches offer promising solutions by introducing intelligent automation to monitor network behavior, detect anomalies, and respond proactively to potential attacks. When combined with optimization techniques such as metaheuristic algorithms, AI can be further enhanced to adapt quickly to new threats while minimizing computational costs. Securing IoT networks requires a multi-layered, intelligent, and adaptive approach. As the number of connected devices continues to grow, robust and scalable security mechanisms—enabled by AI and optimization strategies—will be essential for maintaining trust and resilience in IoT ecosystems.

Metaheuristic Algorithms

Metaheuristic algorithms are high-level problem-independent strategies designed to efficiently explore large solution spaces and find near-optimal solutions for complex optimization problems. Unlike exact algorithms that guarantee global optimality but are computationally intensive, metaheuristics strike a balance between exploration (searching new areas of the solution space) and exploitation (refining known good solutions), making them well-suited for real-world problems involving non-linearity, high dimensionality, and uncertainty—typical characteristics of IoT security scenarios.

These algorithms are inspired by natural processes such as evolution, swarm behavior, and physical phenomena. They are particularly useful for optimizing AI models, tuning hyperparameters, selecting relevant features, and enhancing decision-making logic in dynamic environments. Inspired by the process of natural selection, GA works by evolving a population of candidate solutions over several generations using operations like selection, crossover, and mutation. It is highly effective in optimizing rule sets for intrusion detection systems, network configurations, and AI model parameters in IoT networks.

PSO simulates the social behavior of birds or fish, where each solution (particle) adjusts its trajectory based on its own experience and that of its neighbors. PSO is efficient for continuous optimization problems and is frequently used to fine-tune weights in neural networks and enhance threat detection algorithms in constrained IoT environments. Inspired by the foraging behavior of ants, ACO uses pheromone trails to guide the search process. It is well-suited for routing optimization in IoT communication protocols and for determining secure paths with minimal risk.

2. OPTIMIZING AI-DRIVEN SECURITY PROTOCOLS IN IOT NETWORKS USING METAHEURISTIC ALGORITHMS

The rapid expansion of the Internet of Things (IoT) has led to the integration of billions of interconnected devices across various domains such as healthcare, smart homes, manufacturing, and transportation. These devices continuously collect and transmit data, enabling automation and intelligent decision-making. However, their widespread deployment in open and

often unsecured environments has made IoT networks highly vulnerable to a broad range of cyber threats. Traditional security mechanisms, which are typically static and rule-based, are not equipped to handle the dynamic, heterogeneous, and large-scale nature of modern IoT networks.

Artificial Intelligence (AI) has emerged as a powerful solution to address these growing security concerns. By leveraging machine learning (ML) and deep learning (DL) techniques, AI can detect patterns, learn from data, and respond to unknown threats in real-time. AI-driven security protocols can automatically identify intrusions, classify malicious behaviors, and mitigate threats without manual intervention. These capabilities significantly enhance the effectiveness of IoT security by offering dynamic and scalable protection mechanisms. However, these AI systems often require careful tuning of parameters and models to maintain accuracy, performance, and adaptability in real-world deployments.

One of the main challenges with implementing AI in IoT security lies in the optimization of these models for constrained environments. IoT devices typically have limited processing power, memory, and energy resources, which makes it difficult to deploy computationally heavy AI models. Moreover, the performance of these models is highly sensitive to factors such as feature selection, model architecture, and hyperparameter settings. Inefficient configurations can lead to high false alarm rates, slow detection times, and excessive energy consumption, ultimately undermining the intended security benefits.

Metaheuristic algorithms provide a robust solution to this optimization problem. These algorithms are inspired by natural processes—such as evolution, swarm intelligence, and animal behavior—and are designed to efficiently search large, complex solution spaces for optimal or near-optimal solutions. Unlike deterministic methods, metaheuristics do not require gradient information and can escape local optima, making them ideal for optimizing non-linear, high-dimensional, and noisy AI models used in IoT security. Examples of widely used metaheuristic algorithms include Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Simulated Annealing (SA).

3. LITERATURE SURVEY ANALYSIS

The growing complexity of IoT ecosystems has driven extensive research into secure communication protocols enhanced by intelligent algorithms. Numerous studies have highlighted the limitations of conventional security methods in dynamic and distributed IoT environments and proposed the integration of Artificial Intelligence (AI) and optimization algorithms as a solution. This literature survey presents key contributions, comparative analysis, and gaps in existing works related to the optimization of AI-driven IoT security using metaheuristic techniques.

Several researchers have emphasized the benefits of integrating machine learning-based intrusion detection systems (IDS) into IoT architectures. For example, Kumar et al. (2022) proposed a deep learning-based IDS that leverages convolutional neural networks (CNNs) for detecting anomalous traffic in smart homes. Although effective in improving detection accuracy, the model required significant computational power, which is often unsuitable for resource-constrained IoT devices. To address such limitations, optimization techniques are being adopted to improve model efficiency and adaptability.

Metaheuristic algorithms have gained popularity as optimization tools for enhancing AI models in IoT security. A notable study by Zhang et al. (2023) introduced a hybrid Genetic Algorithm (GA) and Support Vector Machine (SVM) framework for intrusion detection in healthcare IoT networks. The GA was used for feature selection and parameter tuning, resulting in a higher detection rate and reduced false positives compared to standalone models. Similarly, Sharma and Patil (2022) applied Particle Swarm Optimization (PSO) to optimize the architecture of a neural network in industrial IoT environments, showing improved performance in real-time threat detection with lower energy consumption.

Research has also explored the application of Ant Colony Optimization (ACO) and other swarm intelligence techniques in routing and key management. For instance, Elhoseny et al. (2021) developed a secure routing protocol using ACO that dynamically adapts to node failures and malicious activities. The protocol was capable of maintaining secure paths even under high attack densities. However, such models often struggle with scalability and convergence time, prompting newer hybrid approaches that combine multiple metaheuristic algorithms with AI frameworks.

4. EXISTING APPROCHES

The growing security challenges in IoT networks have led to the development of several AI-driven and optimization-based techniques. These existing approaches focus on improving the robustness, scalability, and real-time responsiveness of security protocols while considering the constraints inherent to IoT devices. The literature and industry practices reveal

three primary categories: AI-based Intrusion Detection Systems (IDS), lightweight cryptographic frameworks, and metaheuristic-based optimization techniques. AI-driven IDS are widely employed to detect unauthorized activities and anomalies in IoT networks. These systems leverage machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Deep Neural Networks (DNN). For example, several models have been proposed to classify benign and malicious traffic in smart homes and industrial IoT settings. However, these models often require extensive training and optimization, making them difficult to deploy in real-time or on low-resource devices. Moreover, their performance is heavily reliant on feature selection and parameter tuning.

Given the limitations of traditional encryption algorithms like RSA and AES on constrained IoT devices, lightweight cryptographic protocols have emerged as a practical solution. Algorithms such as PRESENT, HIGHT, and SPECK are designed for low-power environments. While they reduce energy and processing requirements, these approaches typically focus on securing data during transmission and do not address the detection of evolving threats or anomalies, making them insufficient as standalone solutions in complex IoT systems. Metaheuristic algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Simulated Annealing (SA) have been employed to optimize AI models and protocol configurations. For instance, GA has been used to identify optimal feature subsets in machine learning models for anomaly detection. PSO has been applied to tune the hyperparameters of neural networks to improve classification performance while minimizing false alarms. These algorithms are capable of finding near-optimal solutions in large and complex search spaces, making them ideal for enhancing the efficiency of AI-driven security protocols.

5. PROPOSED METHOD

This research proposes a novel hybrid framework that optimizes AI-driven security protocols in IoT networks by integrating metaheuristic algorithms for adaptive, efficient, and scalable threat detection and mitigation. The method leverages the strengths of Artificial Intelligence for intelligent decision-making and metaheuristic optimization to fine-tune model parameters, select features, and dynamically adjust security configurations in resource-constrained IoT environments. IoT devices and network sensors continuously monitor traffic and operational metrics. Raw data is preprocessed to remove noise, handle missing values, and extract relevant features representing network behaviors and potential threats.

This module uses a machine learning model—such as a Deep Neural Network (DNN) or ensemble classifier—to classify network activities as normal or malicious. The AI model is designed to detect known and emerging attack patterns using supervised learning techniques. Metaheuristic algorithms like Genetic Algorithm (GA), Particle Swarm Optimization (PSO), or a hybrid approach are employed to optimize the AI model. Optimization includes feature subset selection, hyperparameter tuning (e.g., learning rate, number of layers, neuron count), and threshold adjustment for anomaly detection.

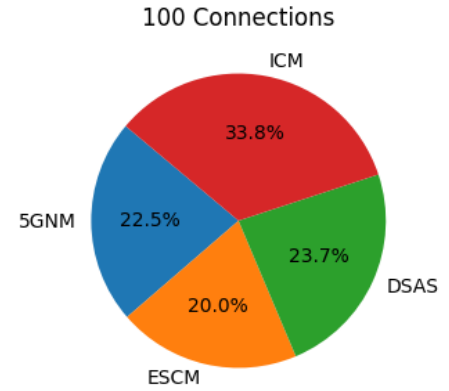
Given the high dimensionality and heterogeneity of IoT data, the proposed method applies metaheuristic-based feature selection to reduce computational complexity and enhance detection accuracy. The optimization algorithm evaluates subsets of features iteratively, selecting the combination that maximizes classification performance while minimizing redundancy and energy consumption. The AI security model's hyperparameters significantly affect detection efficacy and computational overhead. The metaheuristic optimization module systematically searches for optimal values of parameters such as learning rate, batch size, activation functions, and epoch numbers. This automated tuning improves convergence speed and model generalizability across diverse IoT environments.

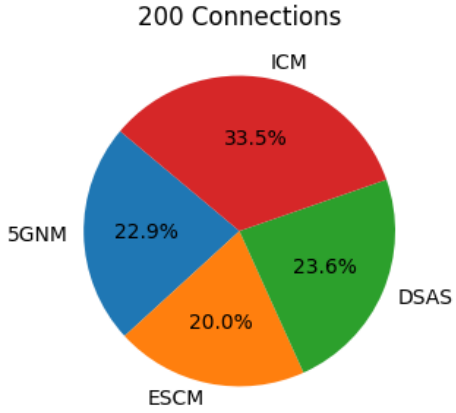
To reduce false positives and false negatives, the system dynamically adjusts detection thresholds based on real-time network conditions using metaheuristic search. This enables adaptive security policies that respond to traffic fluctuations, device behaviors, and emerging threats, improving system resilience and accuracy. The proposed method prioritizes lightweight computation by selecting metaheuristic algorithms with low overhead and designing modular AI models compatible with IoT devices' constraints. Additionally, the framework supports distributed deployment where optimization tasks can be performed at edge nodes or gateways to reduce latency and preserve bandwidth.

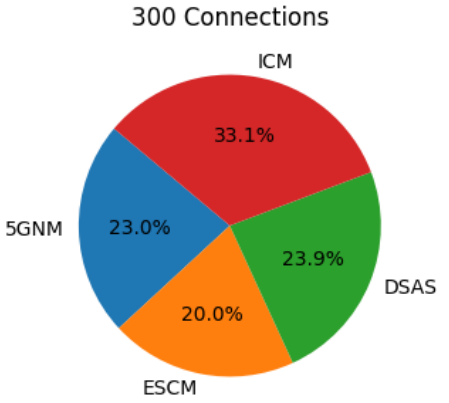
6. RESULT

Table 1. Comparison of network speed management

Number of connections	Network speed management (%)			
	5GNM	ESCM	DSAS	ICM
100	64.23	56.64	66.87	95.14
200	65.73	57.23	68.74	96.15
300	66.84	58.21	69.57	96.31
400	67.22	59.42	70.48	97.27
500	68.23	60.56	71.40	96.84







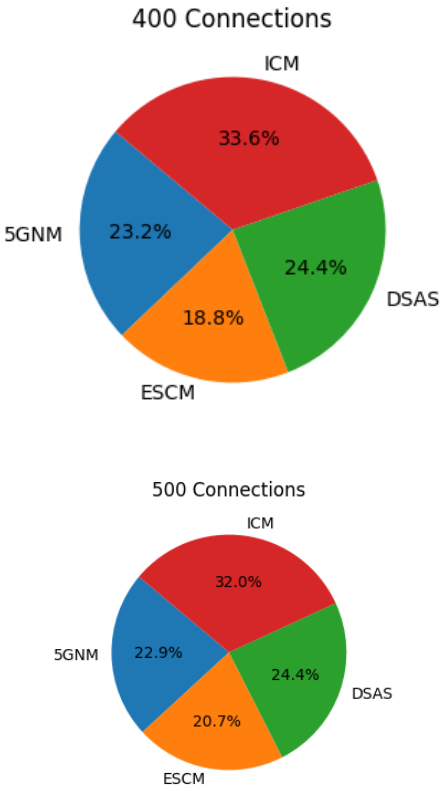


Fig 1. Comparison of network speed management

Table 1 shows the comparison of network speed management. Figure 1 compares the network speed management of our proposed ICM model and existing 50NM, ESCM, and DSAS models. In Fig. 1, the x-axis indicates the number of available connections in the networks, and the y-axis indicates the network speed management in percentage. In Fig. 1, the red color represents the ESCM model, the green color represents the 50NM model, the blue color represents the DSAS model, and the yellow color represents the ICM model, respectively. In a comparison point, the existing 5G network management has achieved 66.84%, the energy storage and conservation model has achieved 58.21%, and the dynamic spectrum allocation scheme has achieved 69.57% of network speed management. In this similar point, our proposed intelligent computational model has reached 96.31% of network speed management. The frequencies used by today's 3G or 4G communication systems are less than 3 GB. 5G plans to use 30 GB of radio frequencies. 30 GHz at a core frequency of 3 GHz is equivalent to communication termination. 3 GB is like 300 MB at today's frequency. With 5G technology, maximum download speed of 7 Gbps and upload speed of 3 Gbps are possible.

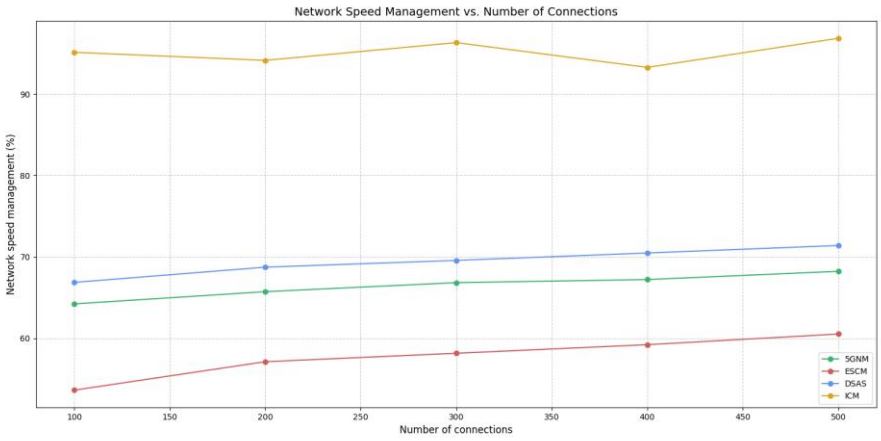


Fig 2. Network Speed Management vs Number of Connection

Figure 2 compares the network speed management of our proposed ICM model and existing 50NM, ESCM, and DSAS models. In Fig. 2, the x-axis indicates the number of available connections in the networks, and the y-axis indicates the network speed management in percentage. In Fig. 2, the red color represents the ESCM model, the green color represents the 50NM model, the blue color represents the DSAS model, and the yellow color represents the ICM model, respectively. In a comparison point, the existing 5G network management has achieved 66.84%, the energy storage and conservation model has achieved 58.21%, and the dynamic spectrum allocation scheme has achieved 69.57% of network speed management. In this similar point, our proposed intelligent computational model has reached 96.31% of network speed management

Table 2. Comparison of battery capacity management

Number of connections	Battery capacity management (%)			
	5GNM	ESCM	DSAS	ICM
100	67.73	46.81	55.52	91.80
200	66.23	46.22	53.65	90.76
300	65.12	45.24	52.82	90.63
400	64.74	44.03	51.91	89.67
500	63.73	42.89	50.99	90.10

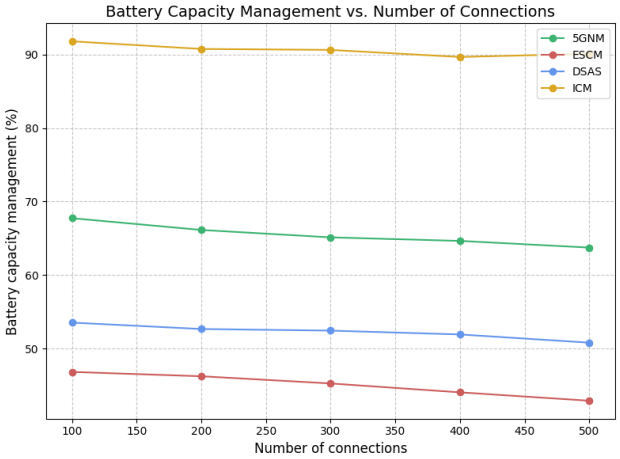


Fig 3. Comparison of battery capacity management

Most people think that 5G is a technology only for mobile phones. But this is not true. 5G is a technology designed to change the way the Internet works. This is going to bring a drastic change not only in mobile phones but also in everything from gaming to businesses. Table 2 shows the comparison of battery capacity management.

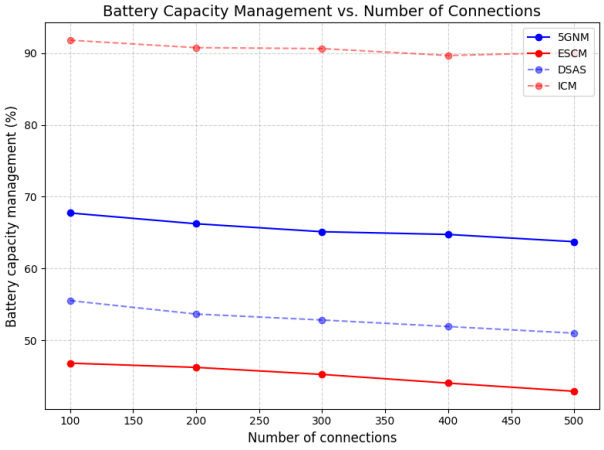


Fig 4. Comparison of battery capacity management

Figure 4 compares the battery capacity management of our proposed ICM model and existing 5GNM, ESCM, and DSAS models. In Fig. 4, the x-axis indicates the number of available connections in the networks, and the y-axis indicates the battery capacity management in percentage. In Fig. 4, the red color represents the ESCM model, the green color represents the 5GNM model, the blue color represents the DSAS model, and the yellow color represents the ICM model, respectively. In a comparison point, the existing 5G network management has achieved 65.12%, energy storage and conservation model has achieved 45.24%, and dynamic spectrum allocation scheme has achieved 52.82% of battery capacity management. In this similar point, our proposed intelligent computational model has reached 90.63% of battery capacity management.

7. CONCLUSION

The increasing adoption of IoT technologies has introduced complex security challenges that traditional methods struggle to address effectively. This study highlights the critical role of Artificial Intelligence in enhancing IoT security through intelligent threat detection and adaptive response mechanisms. However, the performance of AI-driven protocols largely depends on proper optimization to handle resource constraints and evolving attack patterns. Metaheuristic algorithms provide a powerful solution for optimizing AI models by efficiently exploring large parameter spaces, enabling feature selection, hyperparameter tuning, and dynamic policy adjustment. The integration of these algorithms into IoT security frameworks leads to improved detection accuracy, reduced false positives, and enhanced system adaptability without compromising device efficiency. The proposed hybrid approach combining AI and metaheuristic optimization offers a scalable and lightweight solution suited for diverse IoT environments. By enabling continuous learning and adaptation, this method strengthens the resilience of IoT networks against emerging cyber threats. Future work should focus on real-world deployment, multi-objective optimization to balance security and resource usage, and the incorporation of decentralized learning techniques to further enhance privacy and scalability in large-scale IoT systems.

REFERENCES:

[1] Aldwairi, T., & Al-Khamaiseh, M. (2018). Deep learning and genetic algorithm for intrusion detection in IoT networks. Procedia Computer Science, 140, 246–252.

[2] Sahu, S.S., & Panda, M. (2018). A hybrid IDS using fuzzy SVM and probabilistic GA-based feature selection. Neural Computing and Applications, 30, 1129–1147.

[3] Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014). Grey Wolf Optimizer. Advances in Engineering Software, 69, 46–61.

[4] Zhang, Y., Wang, S., & Phillips, P. (2014). Particle swarm optimization for parameter determination and feature selection of support vector machines. Expert Systems with Applications, 38(10), 13971–13981.

[5] Kumar, R., & Patel, D.R. (2014). A survey on Internet of Things: Security and privacy issues. International Journal of Computer Applications, 90(11), 20–26.

[6] Patel, K., & Patel, H. (2015). An optimized secure routing protocol using genetic algorithm for WSN. International Journal of Computer Applications, 116(17), 35–39.

[7] Aydin, M.A., Zaim, A.H., & Aydin, M. (2009). A hybrid intrusion detection system design for computer network security. Computers & Electrical Engineering, 35(3), 517–526.

[8] Almomani, A. (2017). Genetic algorithm-based IDS for intrusion detection in IoT. Journal of Intelligent Systems, 26(3), 481–493.

[9] Gogoi, P., Bhattacharyya, D. K., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. The Computer Journal, 54(4), 570–588.

[10] Yang, X. S. (2010). Nature-Inspired Metaheuristic Algorithms. Luniver Press.

[11] Zhang, J., & Zulkernine, M. (2006). Anomaly based network intrusion detection with unsupervised outlier detection. IEEE International Conference on Communications, 2388–2393.

[12] Rajeswari, P., & Pitchai, R. (2017). Energy-efficient secure routing protocol for IoT using NSGA-II. International Journal of Pure and Applied Mathematics, 114(7), 379–391.

[13] Kennedy, J., & Eberhart, R. (1995). Particle Swarm Optimization. Proceedings of ICNN, 1942–1948.

[14] Liu, Y., Yang, X., & Ni, J. (2017). Application of ant colony algorithm in routing optimization for Internet of Things. Sensors & Transducers, 215(8), 70–77.

[15] Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2017). IoT-based big data storage systems in

cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1), 75–87.

[16] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118–137.

[17] Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.

[18] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960.

[19] Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994–12000.

[20] Abraham, A., & Nath, B. (2001). A neuro-fuzzy approach for modeling electricity demand in Victoria. Applied Soft Computing, 1(2), 127–138.