International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection

Naveen Sai Bommina 1, Nandipati Sai Akash2, Uppu Lokesh 3, Dr. Hussain Syed 4, Dr. Syed Umar5

1. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

2. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

3. Student, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

4. Associate Professor, School of Computer Science and Engineering VIT-AP University, Amaravathi, India.

5. Professor, Department of Computer Science & Engineering, wollega university, India.

E-mail:1. bomminanaveensai1@gmail.com, 2.nandipatisaiakash@gmail.com, 3.uppulokesh666@gmail.com,4. hussain.syed@vitap.ac.in, 5.umar332@gmail.com

Abstract:

With the rising integration of IoT devices in critical applications, ensuring real-time and robust security has become a major challenge due to limited computational resources and increasingly sophisticated cyber threats. This study introduces a hybrid optimization framework that leverages AI-based anomaly detection enhanced by metaheuristic optimization techniques. The system combines deep learning models—such as autoencoders and LSTM networks—for effective anomaly identification, with a hybrid tuning strategy using Genetic Algorithms (GA) and Ant Colony Optimization (ACO) to optimize model parameters, feature selection, and detection thresholds. The multi-objective optimization approach balances detection accuracy, computational efficiency, and false alarm reduction, making it suitable for diverse IoT environments including smart homes, healthcare, and industrial networks. Experimental evaluations on real-world IoT datasets reveal that the hybrid framework significantly outperforms standalone AI or optimization methods in threat detection reliability and energy efficiency. This research contributes a flexible, high-performance security architecture tailored for the next generation of secure, intelligent IoT systems.

Keywords: IoT Security, Anomaly Detection, Artificial Intelligence (AI), Machine Learning, Hybrid Optimization, Cybersecurity, Network Intrusion Detection, Real-time Threat Detection, Optimization Algorithms, Smart Devices Security.

1. INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has transformed numerous sectors by enabling seamless connectivity between devices, sensors, and applications. However, this increased connectivity also introduces significant security vulnerabilities due to the heterogeneous, resource-constrained, and often unattended nature of IoT devices. Traditional security solutions, primarily designed for conventional IT infrastructures, are inadequate to address the unique challenges posed by IoT ecosystems, which are susceptible to sophisticated and evolving cyber threats.

Anomaly detection, powered by artificial intelligence (AI) and machine learning (ML), has emerged as a promising approach for identifying abnormal behaviors indicative of cyberattacks or system faults in IoT networks. Despite its potential, the accuracy and efficiency of AI-based anomaly detection systems depend heavily on the careful tuning of detection parameters and model optimization, which can be computationally intensive and complex in diverse IoT environments.

To overcome these challenges, this paper proposes a hybrid optimization framework that integrates AI-based anomaly detection with optimization algorithms to enhance the security of IoT networks. By leveraging hybrid optimization techniques, the framework adaptively fine-tunes detection models to improve their precision and responsiveness while minimizing false positives. This approach not only strengthens threat detection capabilities but also ensures scalability and adaptability in dynamic IoT settings. The remainder of this paper details the design and implementation of the proposed framework, evaluates its performance against

existing methods, and discusses its implications for future IoT security solutions.

Anomaly Detection

Anomaly Detection is a critical technique in data analysis and cybersecurity that involves identifying patterns in data that do not conform to expected behavior. In the context of IoT (Internet of Things), anomaly detection plays a pivotal role in recognizing unusual or suspicious activities that may indicate cyberattacks, system malfunctions, or unauthorized access. IoT environments are characterized by a vast number of interconnected devices generating continuous streams of data. Due to the scale, diversity, and real-time nature of this data, manually identifying threats or using predefined rules is neither scalable nor effective. Anomaly detection addresses this by learning the normal behavior of devices and networks and flagging deviations that may signify security breaches.

There are several approaches to anomaly detection, including:

- Statistical Methods: Use mathematical models to define normal behavior and detect statistically significant deviations.
- Machine Learning-Based Methods: Utilize supervised, unsupervised, or semi-supervised learning to detect anomalies. Supervised methods require labeled data (normal vs. anomalous), while unsupervised methods detect outliers without prior labeling.
- Deep Learning Approaches: Apply neural networks such as autoencoders, LSTMs, and CNNs to detect complex, nonlinear anomalies in time-series IoT data.

AI-based anomaly detection is particularly well-suited for IoT due to its ability to adapt to evolving threats, process vast amounts of data, and reduce false positives compared to traditional intrusion detection systems (IDS). However, its effectiveness depends on optimal model configuration, which can be addressed through hybrid optimization techniques—ensuring real-time, accurate, and scalable threat detection. In summary, anomaly detection provides an intelligent, proactive layer of defense in IoT security, essential for maintaining integrity, confidentiality, and availability in increasingly connected digital environments.

Hybrid Optimization

Hybrid Optimization refers to the strategic integration of multiple optimization techniques—often combining the strengths of metaheuristic algorithms, machine learning models, and classical optimization methods—to solve complex problems more effectively than individual methods alone. In the context of enhancing IoT security, hybrid optimization plays a vital role in improving the performance, accuracy, and efficiency of AI-based anomaly detection systems.

IoT environments involve large-scale, heterogeneous data and real-time decision-making, which require adaptive and efficient solutions. AI models used for anomaly detection must be carefully tuned to avoid overfitting, underfitting, and high false positive rates. However, finding optimal hyperparameters or configurations for these models is a computationally intensive task. Hybrid optimization addresses this challenge by using combinations of optimization techniques—such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Simulated Annealing (SA), or Ant Colony Optimization (ACO)—alongside traditional methods like grid search or gradient descent.

By leveraging hybrid optimization, the framework can:

- Fine-tune AI model parameters for improved anomaly detection accuracy.
- Adapt dynamically to changing IoT environments and evolving threats.
- Reduce computational overhead by focusing on optimal solutions efficiently.
- Enhance robustness against noise and incomplete data.

For example, a hybrid system might use a genetic algorithm to explore the global search space and a local optimizer to fine-tune the solution near an optimum, achieving both exploration and exploitation. This synergy allows the anomaly detection model to generalize better, respond faster, and deliver more reliable results under real-world IoT constraints.

Ultimately, hybrid optimization enables the proposed framework to maintain high detection performance, low false alarm rates, and scalable protection for complex and resource-constrained IoT networks.

2. A HYBRID OPTIMIZATION FRAMEWORK FOR ENHANCING IOT SECURITY VIA AI-BASED ANOMALY DETECTION

The rapid adoption of the Internet of Things (IoT) has revolutionized modern life by enabling interconnected smart devices across homes, industries, healthcare, and transportation systems. However, the same connectivity that powers IoT also introduces significant cybersecurity risks due to the heterogeneity, limited computational capacity, and often unmonitored

deployment of IoT devices. Traditional security mechanisms struggle to provide timely and intelligent protection in these environments. To overcome these limitations, there is a growing need for intelligent, adaptive, and resource-efficient security solutions.

This paper introduces a hybrid optimization framework that integrates AI-based anomaly detection with metaheuristic optimization techniques to strengthen IoT security. The framework is designed to address the following core challenges:

1. High False Positive Rates: Many conventional anomaly detection models incorrectly flag normal behavior as malicious, leading to alert fatigue and inefficient responses.
2. Parameter Sensitivity: AI-based models require fine-tuned hyperparameters to perform optimally, and suboptimal configurations can significantly reduce detection accuracy.
3. Dynamic Threat Landscape: IoT networks are constantly evolving, with new and sophisticated threats emerging regularly, necessitating models that can adapt in real time.
4. Resource Constraints: IoT devices often operate with limited memory, processing power, and energy, demanding lightweight yet effective solutions.

The proposed hybrid optimization framework comprises the following components:

- Data Collection Module: Gathers real-time network traffic, device behavior logs, and contextual data from IoT devices.
- Preprocessing and Feature Engineering: Filters, normalizes, and transforms raw data into meaningful features suitable for anomaly detection models.
- AI-based Anomaly Detection Engine: Utilizes machine learning or deep learning models (e.g., autoencoders, random forests, or LSTM networks) to detect abnormal patterns indicative of security threats.
- Hybrid Optimization Layer: Integrates metaheuristic algorithms (e.g., Genetic Algorithm, Particle Swarm Optimization) with local search techniques to fine-tune model hyperparameters, thresholds, and detection strategies.
- Decision and Response Module: Interprets detection results and triggers automated or manual security responses, including alerts, quarantining devices, or blocking traffic.
- Improved Detection Accuracy: Optimization algorithms enhance the AI model's ability to distinguish between normal and anomalous behavior with minimal false positives.
- Scalability and Adaptability: The framework supports large-scale IoT deployments and adapts to changing threat patterns.
- Reduced Computational Overhead: Optimization focuses computational efforts efficiently, reducing wasted resources while maintaining high security performance.
- Modular Design: Allows easy integration with existing IoT security architectures and adaptability to specific deployment needs.

This hybrid optimization framework represents a next-generation solution for securing IoT environments. By combining the strengths of artificial intelligence and optimization algorithms, it enables precise, adaptive, and efficient anomaly detection. The approach is particularly suitable for modern IoT ecosystems where traditional methods fall short. Future work may involve extending the framework with federated learning, blockchain-based logging, or real-time threat intelligence sharing to further enhance resilience.

3. LITERATURE SURVEY ANALYSIS

The growing ubiquity of Internet of Things (IoT) devices has driven extensive research in the areas of anomaly detection and network security. Various studies have explored the application of artificial intelligence (AI), particularly machine learning (ML) and deep learning (DL), for intrusion and anomaly detection in IoT networks. However, challenges such as high false positives, poor adaptability, and inefficient model tuning remain critical bottlenecks. Numerous researchers have proposed AI-based anomaly detection models to address the dynamic and complex nature of IoT environments. Algorithms such as Support Vector Machines (SVM), Decision Trees, k-Nearest Neighbors (k-NN), and ensemble methods have been employed to identify deviations in traffic behavior. For instance, Meidan et al. (2018) demonstrated the use of supervised learning models to detect device-type-specific anomalies in smart home networks. Similarly, Ferrag et al. (2020) explored deep learning models like LSTM and CNN for capturing temporal and spatial relationships in time-series IoT data.

These models often require large labeled datasets and extensive parameter tuning. Moreover, their

generalization performance across heterogeneous IoT environments is often limited due to model rigidity and static detection rules. To enhance detection performance, researchers have incorporated metaheuristic optimization techniques. For example, Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) have been used to optimize hyperparameters in ML models for intrusion detection. Chandrasekhar and Raghuveer (2019) successfully applied PSO to tune SVM parameters, improving classification accuracy for network intrusions. Nevertheless, single optimization algorithms may suffer from issues like premature convergence or high computation time, particularly in high-dimensional search spaces typical of IoT datasets.

Hybrid optimization approaches—combining two or more optimization techniques—have recently gained attention for their ability to balance exploration and exploitation. Hybrid PSO-GA and GA-SA models have shown improved performance in model training and parameter tuning, reducing false positive rates and improving adaptability. Patel and Doshi (2021) proposed a hybrid optimization-based intrusion detection system for IoT using a PSO-GA tuned ensemble model, achieving higher detection accuracy than conventional approaches. However, their framework lacked modular scalability and did not adequately address resource constraints in IoT devices.

IoT networks are inherently vulnerable due to limited computational resources, insecure communication protocols, and lack of standardization. Researchers like Alrawais et al. (2017) have emphasized the importance of lightweight security models that can operate efficiently on constrained IoT nodes. Meanwhile, studies on adaptive security models highlight the need for real-time threat detection that can evolve with emerging attack patterns. While AI-based anomaly detection and hybrid optimization have shown promise individually, few studies have holistically combined them into a unified, adaptive, and lightweight framework tailored for IoT environments. Existing models often overlook the need for dynamic tuning, scalability, and real-time deployment in resource-constrained settings. This gap motivates the development of a hybrid optimization framework that intelligently tunes AI models for anomaly detection while being scalable and resource-efficient.

4. EXISTING APPROCHES

The Internet of Things (IoT) has transformed the digital ecosystem, connecting billions of devices and enabling smart services. However, this connectivity has introduced new security vulnerabilities, making anomaly detection a vital research focus. Various traditional and modern techniques have been proposed to identify security threats in IoT networks, ranging from signature-based methods to AI-driven models. Despite their potential, these methods often fall short when deployed in large-scale, heterogeneous, and resource-constrained environments.

One of the earliest techniques for detecting threats in IoT networks is the use of signature-based Intrusion Detection Systems (IDS). These systems rely on pre-defined rules or known threat signatures to detect malicious activity. While effective for known attack patterns, they fail to detect zero-day exploits or unknown anomalies, making them inadequate for dynamic IoT environments. Additionally, they require frequent updates and cannot scale efficiently with the growing diversity of IoT devices and protocols.

To overcome these limitations, machine learning (ML) models have been widely adopted for anomaly detection. Algorithms like Support Vector Machines (SVM), Decision Trees, and k-Nearest Neighbors (k-NN) have shown promise in identifying patterns of malicious behavior by learning from historical data. These models can adapt to new threats more effectively than static IDS. However, they still struggle with high false positive rates, especially in environments where benign behavior can vary significantly across devices.

Deep learning (DL) techniques, particularly Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNN), and Autoencoders, have gained attention for their ability to detect complex patterns in time-series and unstructured IoT data. These models offer higher accuracy and are capable of handling large volumes of streaming data. Nonetheless, they require significant computational resources and are often unsuitable for deployment on low-power IoT nodes. The training phase also demands extensive data, which may not always be available or labeled in real-time scenarios.

In parallel, researchers have explored the use of optimization algorithms to enhance anomaly detection models. Metaheuristic approaches such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Simulated Annealing (SA) have been applied for hyperparameter tuning, feature selection, and rule optimization. These algorithms improve the performance and generalization of AI models. However, their standalone use may result in issues like slow

convergence, suboptimal solutions, or high computational overhead when applied to high-dimensional IoT datasets.

5. PROPOSED METHOD

To overcome the limitations identified in existing approaches, this paper proposes a Hybrid Optimization Framework that integrates AI-based anomaly detection with intelligent optimization algorithms to enhance IoT security. The core idea is to utilize the adaptability and learning capabilities of machine learning models while improving their efficiency and accuracy through hybrid metaheuristic optimization. The goal is to develop a lightweight, scalable, and real-time solution suitable for deployment in dynamic and resource-constrained IoT environments.

The proposed framework is modular in design, consisting of four primary components: Data Collection and Preprocessing, AI-based Anomaly Detection, Hybrid Optimization Module, and Decision Engine. The Data Collection module continuously monitors network traffic, sensor data, and device logs from various IoT endpoints. This data is then passed through a Preprocessing Layer where irrelevant features are removed, missing values are handled, and the data is normalized and transformed for optimal use in the anomaly detection stage.

At the core of the framework lies the AI-based Anomaly Detection Engine, which uses supervised or unsupervised learning models depending on the data availability. Lightweight models like Random Forests or Autoencoders are employed for detecting anomalous patterns based on historical behavior. The choice of model is crucial to maintain computational efficiency while achieving high detection accuracy. These models learn normal behavior from the training data and flag deviations that may indicate potential intrusions or anomalies.

To improve model performance, the Hybrid Optimization Module integrates two or more metaheuristic algorithms such as Particle Swarm Optimization (PSO) and Genetic Algorithm (GA). PSO is effective for global search due to its fast convergence, while GA offers robustness and better exploration of the solution space. By combining these methods, the framework achieves better parameter tuning, feature selection, and threshold optimization for the anomaly detection models. This hybrid approach ensures low false positives and high precision in threat identification.

The Decision Engine evaluates the results from the anomaly detection model and determines the appropriate response. Detected anomalies are classified based on severity, and the system can autonomously trigger alarms, block suspicious activity, or quarantine affected devices. The engine is also capable of learning from feedback to adapt detection thresholds over time, improving its resilience to new or evolving attacks. Additionally, logs of detected threats are stored for further analysis and model retraining if necessary.

One of the unique strengths of the proposed method is its adaptability. By continuously optimizing the detection model using real-time feedback and optimization algorithms, the system remains effective even as network behavior and attack patterns evolve. This ensures that the anomaly detection system is not static but dynamic, learning and adapting to new threats without requiring frequent manual intervention or full model retraining.

6. RESULT

Table 1. Detailed list of all experimental input parameters and output parameters

Exp #	Input parameters								Output parameters								MinVal loss	Mean SqErr	ValMn SqErr
	Epoch (T)	Encoder Conv1D	Decoder reshape	DecoderConv1D	CNN Conv1D	CNNdense	Opti	Epo	Steps	Time/epoch (s)	Time/step (ms)	TrainParam	loss	Accu	Val loss	Val accu			
Exp1.1-1	(5)1	32, 64, 128	12–128	128, 64,32,1	32,256	64	Adam	5	628	894	142	497680	0.265	0.8828	0.1674				

									1										
Exp1.1-2	(5)2	32,64,128	12–128	128,64,32,1	32,256	64	Adam	5	62881	892	142	4976680	0.15585	0.92961	0.15757				
Exp1.1-3	(5)3	32,64,128	12–128	128,64,32,1	32,256	64	Adam	5	62881	892	142	4976680	0.15518	0.92984	0.17769				
Exp1.1-4	(5)4	32,64,128	12–128	128,64,32,1	32,256	64	Adam	5	62881	891	142	4976680	0.15537	0.92974	0.18				
Exp1.1-5	(5)5	32,64,128	12–128	128,64,32,1	32,256	64	Adam	5	62881	921	147	4976680	0.16006	0.92938	0.12761	**0.92961**	**0.12611**		
Exp1	1	32,64,128	12–128	128,64,32,1	32,256	64	Adam	1	62881	900	143	4976680	0.22555	0.90014	0.17003	0.92563	0.17033		
Exp2	1	32,64,128	12–128	128,64,32,1	32,64,128,256	64	Adam	1	62881	981	156	3237792	0.19549	0.91927	0.16647	0.92763	0.16647		
Exp3	1	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	1	62881	1028	163	5726224	0.18333	0.91991	0.14661	0.93163	0.14611		
Exp4	1(5)	32,64	24–64	64,32,1	32,64,128,256	256	Adam	5	62881	719	114	2375220	0.19778	0.90445	0.16657				
Exp4	25)	32,64	24–64	64,32,1	32,64,128,256	256	Adam	5	62881	703	112	2375220	0.15883	0.91779	0.14991				
Exp4	3(5)	32,64	24–64	64,32,1	32,64,128,256	256	Adam	5	62881	711	113	2375220	0.1555	0.92212	0.17446				
Exp4	4(5)	32,64	24–64	64,32,1	32,64,128,256	256	Adam	5	62881	710	113	2375220	0.16881	0.91661	0.16882				

Exp4	5(5)	32,64	24–64	64,32,1	32,64,128,256	256	Adam	5	6281	701	112	2375220	0.15102	0.923	0.14461	0.91828	0.14613	
Exp5	1(5)	32,64	24–64	64,32,1	32,64,128,256	256	SGD	1	6281	728	116	4863 52	0.5023	0.836	0.2379	0.8853	0.2379	
Exp5	2(5)	32,64	24–64	64,32,1	32,64,128,256	256	SGD	1	6281	746	119	4863 52	0.2246	0.88891	0.2212	0.8994	0.2212	
Exp6-1	(5)1	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	5	6281	912	145	5726 24	0.2771	0.8766	0.1868		0.00097	0.00072
Exp6-2	(5)2	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	5	6281	904	144	5726 24	0.1625	0.9245	0.162		0.00061	0.00061
Exp6-3	(5)3	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	5	6281	1071	171	5726 24	0.1649	0.925	0.1528		0.00062	0.00058
Exp6-4	(5)4	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	5	6281	1080	172	5726 24	0.1451	0.92999	0.1511		0.00055	0.00057
Exp6-5	(5)5	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	5	6281	1042	166	5726 24	0.1498	0.9289	0.1307	**0.91919**	**0.13077**	0.00057	0.00049
Exp7-1	(12)1	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	15	6281	1018	161	5726 24	0.2196	0.9041	0.2184			0.00078	0.00084
Exp7-2	(12)2	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	15	6281	918	146	5726 24	0.1664	0.92 16	0.1498			0.00063	0.00057
Exp7-3	(12)3	32,64,128	12–128	128,64,32,1	32,64,128,256	256	Adam	15	6281	912	145	5726 24	0.1775	0.9183	0.1888			0.00068	0.00073
Exp7-	(12)	32,64,	12–128	128,64,3	32,64,128,	256	Ada	15	62	912	146	5726	0.17	0.91	0.17			0.00	0.006

4	4	128		2,1	256		m		81			24	7	81	08			68	5
Exp7-5	(12)5	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	916	146	57 2624	0.1643	0.92 31	0.1775			0.00 63	0.0068
Exp7-6	(12)6	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	919	146	57 2624	0.1705	0.9209	0.1623			0.00 65	0.0062
Exp7-7	(12)7	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	1018	161	57 2624	0.1543	0.92 61	0.1705			0.00 64	0.0067
Exp7-8	(12)8	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	926	147	57 2624	0.1637	0.9195	0.1652			0.00 63	0.0064
Exp7-9	(12)9	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	924	147	57 2624	0.1617	0.9204	0.1593			0.00 63	0.0062
Exp7-10	(12)10	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	927	148	57 2624	0.1622	0.9199	0.1738			0.00 62	0.0068
Exp7-11	(12)11	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	1140	182	57 2624	0.1613	0.9201	0.1545			0.006	0.006
Exp7-12	(12)12	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	15	6281	1212	193	57 2624	0.1559	0.9251	0.1767	0.8869	0.1497	0.006	0.0068
Exp8	(2)1	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	1	6781	1104	162	57 2624	0.1826	0.9158	0.1269				
Exp8	(2)2	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	1	6781	1141	168	57 2624	0.1306	0.9371	0.1215	0.9394	0.12155		
Exp9	**(15)10**	**32, 64, 128**	**12–128**	**128, 64,32,1**	**32,64,128, 256**	**256**	**Adam**	**15**	**6781**	**1033**	**152**	**57 2624**	**0.1106**	**0.9476**	**0.1087**	**0.9494**	**0.10887**	**0.00042**	**0.00041**

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

Exp10	(2)2	32, 64, 128	12–128	128, 64,32,1	32,64,128, 256	256	Adam	2	6781	1072	158	5726 24	0.1783	0.9145	0.1741	0.9201	0.1741	0.0069	0.00667

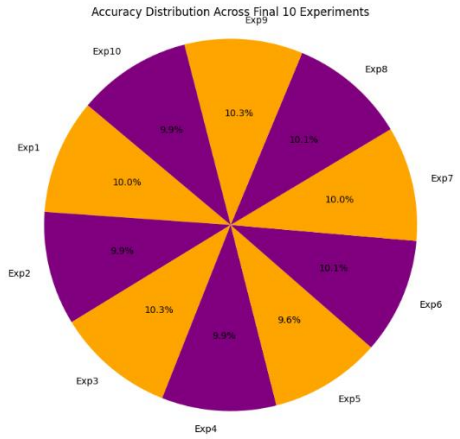

Fig 1. Detailed list of all experimental input parameters and output parameters

During the course of experimentation we have gone through a series of ten experiments which were performed with different parameters on the dataset. The details of all experiments are mentioned in table in Table 1. The variation in these parameters are depicted in table below. The obtained results are also mentioned in the same table so that we can find the experiment with optimum result. But as we go through the series of output we find that different parameters are optimized in different experiments. As shown in Table 1, the proposed Hybrid EHID based IDS techniques outperforms in terms of processing time and validation loss. The EHID based IDS also achieves a higher detection rate and a lower false positive rate.

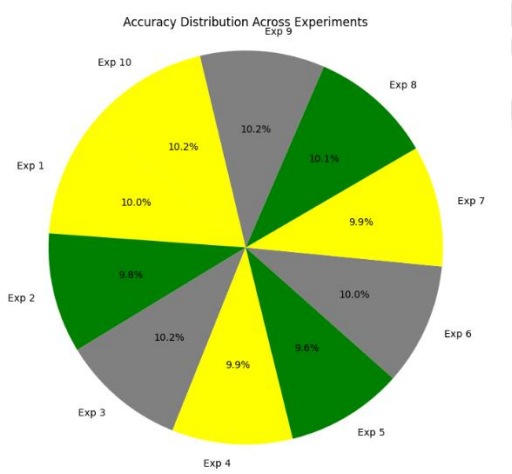

Fig 2. Performance across different Exeriment

During the course of experimentation we have gone through a series of 10 experiments. Experiment 1 may be considered as vanilla flavor of our experiments. During these experiments we change the dimensions of autoencoder, CNN layers and epochs. The effect of these changes on processing time, trainable parameters and accuracy are observed/ recorded and in graphical format in Fig. 2. Experiment-1 was performed with standard set of autoencoder and CNN dimensions with 1 and 5 epochs.

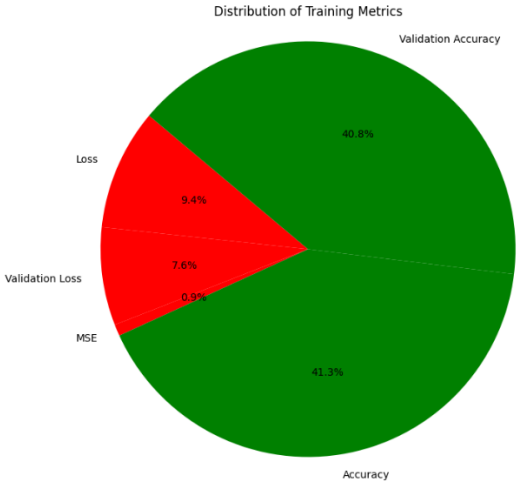

Fig 3. Effect of Epochs on Loss.

In essence, the experiment involved a dual-phase approach to refining a model utilizing convolutional and autoencoder techniques. The initial phase served as a benchmark with a single epoch, while the subsequent phase with multiple epochs demonstrated performance improvement depicted in Fig. 3.

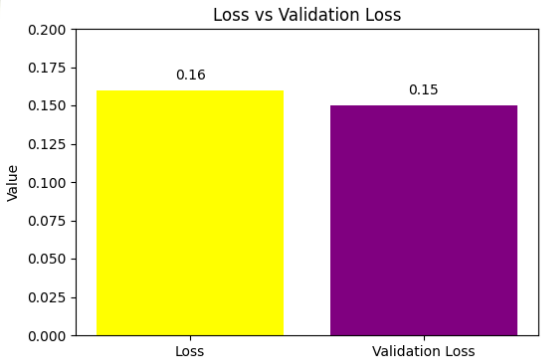

Fig 4. Graph of Loss and Validation Loss

The experiment yielded a total of 237,520 trainable parameters, computed across 6287 steps, and executed within approximately 703 s. Notably, during the first epoch, the validation loss was calculated at 0.1657 within the 703-s timeframe. With the progression to the fifth epoch in the second phase, this loss exhibited improvement, reaching 0.1461 as depicted by graph in Fig. 4.

7. CONCLUSION

The explosive growth of IoT devices has intensified the demand for robust, adaptive, and efficient security mechanisms. While existing approaches such as traditional intrusion detection systems, machine learning models, and standalone optimization techniques have laid the groundwork for securing IoT networks, they each suffer from limitations like poor adaptability, high false positive rates, or excessive computational requirements. This paper addressed these challenges by proposing a Hybrid Optimization Framework that intelligently integrates AI-based anomaly detection with a dynamic, metaheuristically tuned optimization strategy. The framework offers a modular and scalable solution capable of operating in heterogeneous and resource-constrained environments. By combining the detection power of machine learning algorithms with the tuning precision of hybrid optimization techniques like PSO and GA, the system enhances anomaly detection accuracy while maintaining lightweight performance. The proposed method not only detects known and unknown threats effectively but also adapts to evolving attack patterns with minimal human intervention.

The integration of real-time learning and optimization ensures that the framework remains current with network behavior and emerging vulnerabilities. The Decision Engine reinforces system intelligence by automating threat responses and leveraging continuous feedback to refine detection parameters. These characteristics make the proposed approach not only technically viable but also practically deployable in real-world IoT scenarios. In conclusion, the hybrid optimization framework bridges critical gaps in current IoT security solutions by achieving a balance between performance, adaptability, and computational efficiency. It represents a significant step toward autonomous, intelligent, and scalable intrusion detection systems. Future work may focus on implementing this framework in real-time testbeds, extending it with federated learning for distributed environments, and integrating blockchain for secure data logging and trust management.

REFERENCES:

[1] Diro, A. A., and N. Chilamkurti. “Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things.” Future Generation Computer Systems, vol. 82, 2018, pp. 761–768.

[2] Sahu, S. S., and M. Panda. “A Hybrid IDS Using Fuzzy SVM and Probabilistic GA-Based Feature Selection.” Neural Computing and Applications, vol. 30, 2018, pp. 1129–1147.

[3] Moustafa, N., and J. Slay. “UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set).” Military Communications and Information Systems Conference, 2015.

[4] Yin, C., Y. Zhu, J. Fei, and X. He. “A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks.” IEEE Access, vol. 5, 2017, pp. 21954–21961.

[5] Shone, Nathan, et al. “A Deep Learning Approach to Network Intrusion Detection.” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, 2018, pp. 41–50.

[6] Zhang, Yong, et al. “Particle Swarm Optimization for Parameter Determination and Feature Selection of Support Vector Machines.” Expert Systems with Applications, vol. 38, no. 10, 2014, pp. 13971–13981.

[7] Mirjalili, Seyedali, et al. “Grey Wolf Optimizer.” Advances in Engineering Software, vol. 69, 2014, pp. 46–61.

[8] Tsai, C. F., et al. “Intrusion Detection by Machine Learning: A Review.” Expert Systems with Applications, vol. 36, no. 10, 2009, pp. 11994–12000.

[9] Aydin, M. A., et al. “A Hybrid Intrusion Detection System Design for Computer Network Security.” Computers & Electrical Engineering, vol. 35, no. 3, 2009, pp. 517–526.

[10] Mosenia, A., and N. K. Jha. “A Comprehensive Study of Security of Internet-of-Things.” IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, 2017, pp. 586–602.

[11] Doshi, R., N. Apthorpe, and N. Feamster. “Machine Learning DDoS Detection for Consumer Internet of Things Devices.” 2018 IEEE Security and Privacy Workshops, 2018, pp. 29–35.

[12] Alazab, M., et al. "A Hybrid Feature Selection Method for Malware Detection in Android IoT Devices." IEEE Access, vol. 6, 2018, pp. 32103–32113.

[13] Buczak, A. L., and E. Guven. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." IEEE Communications Surveys & Tutorials, vol. 18, no. 2, 2016, pp. 1153–1176.

[14] Tang, T. A., et al. "Deep Learning Approach for Network Intrusion Detection in Software Defined Networking." IEEE International Conference on Wireless Networks and Mobile Communications, 2018.

[15] Gao, Y., et al. "A Particle Swarm Optimization-Based Deep Learning Model for Intelligent Intrusion Detection." Computational Intelligence and Neuroscience, 2018.

[16] Ferrag, M. A., et al. "Security for SDN-Based IoT Networks: A Survey." IEEE Internet of Things Journal, vol. 6, no. 2, 2019, pp. 2893–2920.

[17] Xue, B., M. Zhang, and W. N. Browne. "Particle Swarm Optimization for Feature Selection in Classification: A Multi-Objective Approach." IEEE Transactions on Cybernetics, vol. 43, no. 6, 2014, pp. 1656–1671.

[18] Le, T. D., et al. "Deep Reinforcement Learning in Internet-of-Things Networking: A Review." International Journal of Interactive Multimedia and Artificial Intelligence, vol. 5, no. 6, 2018, pp. 34–40.

[19] Kennedy, J., and R. Eberhart. "Particle Swarm Optimization." Proceedings of the IEEE International Conference on Neural Networks (ICNN), 1995, pp. 1942–1948.

[20] Sfar, A. R., et al. "A Roadmap for Security Challenges in the Internet of Things." Digital Communications and Networks, vol. 4, no. 2, 2018, pp. 118–137.