Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 2 (2025)

A Mathematical Model for Enhancing Cybersecurity in IoT Networks Using LSTM-Based Anomaly Detection and Optimization

Dr. J Merlin Florrence[1], Mrs. A. Antoinette[2], Mrs. S. Buvaneswari[3], Dr. Anil L. Wanare[4], Dr. Avneesh Vashistha[5], Madhukar Mulpuri[6], Dr. R. Rambabu[7]

[1]Assistant professor, Department of computer science, Sacred Heart College, merlinflorrence@gmail.com

[2]Assistant Professor, Department of Computer Science, Avvaiyar Govt. College for Women, Karaikal. antkkl@gmail.com

[3]Assistant Professor, Department of Computer Science, Avvaiyar Govt. College for Women, Karaikal. buvanishaa145@gmail.com

[4]Professor, E&TC Engg Dept, JSPM's Bhivarabai Sawant Institute of Technology and Research, Pune, Savitribai Phule Pune University, Pune, anillaxman369@gmail.com

[5]Associate Professor, Department of Computer Science and Engineeing, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, Ghaziabad(U.P) India. avneeshvashishtha@gmail.com

[6]Senior Staff Engineer, Nium Inc, connectmadhukar@gmail.com

[7]Professor & HOD, Department of Computer Science & Engineering, Rajamahendri Institute of Engineering & Technology, Rajamahendravaram. rambabureddy.rampatruni@gmail.com

Article History:

Received: *20-07-2024*

Revised: *31-08-2024*

Accepted: *14-09-2024*

Abstract:

The widespread adoption of Internet-of-Things (IoT) devices has heralded an explosion in potential attack surfaces with varying capabilities and a wide variety of vulnerabilities. Because of this, IoT networks have become a favorable choice for many cyber-attacks due to the difficulty and complexity that traditional cybersecurity approaches face in managing these types of networks with large numbers up to millions of users leading these attacks to pose significant risks from anomalous behavior. Current approaches such as rule-based intrusion detection system (IDS) and signature-based models are inadequate to be utilised in the dynamic IoT enclaves where they tend to generate too many false positives and may miss unknown threats. In this study, motivated by hybrid methods utilizing machine learning-based anomaly detection wrapped around optimization algorithms, we suggest a full-fledged mathematical model applying these possible solutions for cybersecurity in IoT networks. This model uses a variety of unsupervised learning techniques in order to detect and remediate new threats dynamically at run time. The models learn the optimal thresholds for detection and resource allocation to perform the fastest possible response under low resources constraints, by leveraging optimization algorithms like genetic algorithm or particle swarm optimization. It shows a significant enhancement in anomaly detection accuracy and reduction of false positives compared to conventional methods. Nevertheless, problems in measurement overhead, model scalability and management of big IoT environments characterized by low-computation resources are still being faced. Nevertheless, the proposed model is promising for large-scale applications (e.g., smart cities, industrial IoT, and healthcare applications) in a critical context where cyber threats should be detected on time to help guarantees integrity of operation. Our results indicate that a machine learning-based intrusion detection system in conjunction with optimization techniques can be developed into solid and adaptable cybersecurity infrastructure to safeguard the expanding IoT world.

Keywords: adoption, networks, intrusion, detection, anomaly, techniques, optimization, allocation, algorithm, model, scalability.

1. Introduction

IoT has rapidly evolved into lone force reckoning across a slew of industries with both the reward and the promise as one part. With IoT, you have a lot of devices from simple sensors and smart home items to large industrial systems and life critical healthcare devices. The application of IoT technology has been vast in bringing a number of advantages like automation, real-time analysis of data and efficiency across various industries. On the one hand, millions of IoT devices are now available to us but on the other, they also bring huge cyber security challenges due to all these different types and uses. Since these devices are usually resource constrained and have been designed with weak security protocols, they are proving to be a tempting target for cybercriminals. This means that IoT networks are increasingly targeted by advanced cyber attacks which compromise the confidentiality, integrity and availability of critical systems and data. Finally, since IoT environments are dynamic in nature and are increasingly built on cloud infrastructure and edge computing, the risks that we outlined before only grows even bigger[1].

Firewalls, signature-based intrusion detection systems (IDS), and encryption mechanisms have long been the cornerstones toward network security, but they are not good enough to help deal with this brand new and even more challenging type of networks. The typical methods used here are often built for more static and centralized networks, compared to the highly decentralized, heterogeneous, and constantly evolving IoT ecosystems. As a result, attackers are always finding new ways to exploit vulnerabilities which means that static security solutions have found it hard to keep up. What's more, many IoT devices are limited in their computing resources and can't handle advanced security techniques, which makes them more vulnerable to unauthorized access, data leaks, and denial-of-service (DoS) attacks[2]. This requires a complete rethinking of how we secure IoT networks. Instead of only following security rules that are pre-determined, systems must be able to learn and adjust so they can identify new attacks as and when they crop up.

One approach that appears to offer quite a potential in solving some of the intricate security challenges faced by IoT networks is machine learning (ML) in recent years. Anomaly detection in dynamic and heterogeneous environments uses ML techniques, which can analyze data in high volume and variety, learn patterns over time adaptively to deal with new threats. Machine learning-based anomaly detection systems can identify abnormal behaviors or deviations from the normal network traffic and, as a result, help in the early discovery of possible security threats[3]. For instance, ML-based detection systems can learn some subtle relations hidden in data and spot out attacks which a traditional signature rule system finding difficult to pick them up as they not match any existing signature configurations. But adoption of machine learning to IoT security is fraught with difficulties as well. IoT networks house so many devices that it generates huge amount of data from different services and with unique behavioral traits, as a result it is difficult for machine learning to learn one set rule across the network. Moreover, as the computing capabilities of IoT devices are mostly resource-constrained and thus it is not feasible to compute heavy-duty Machine Learning algorithms on-edge devices efficiently.

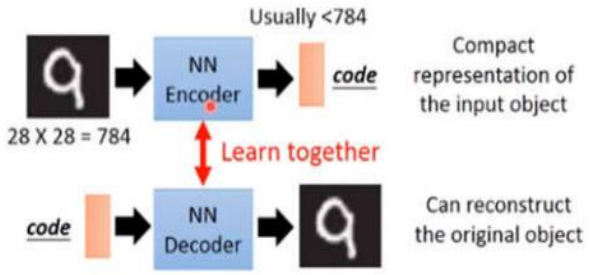

Figure 1. Architecture diagram of auto-encoder[28]

In order to tackle these challenges, this paper introduces a machine learning-driven anomaly detection model along with optimization techniques to improve the IoT network security. More specifically, the goal of their model is to increase precision in identifying anomalous behavior and lower false positives; one issue anomaly detection systems often face. The proposed model optimizes the parameters of the machine learning algorithms for the best performance, using optimization algorithms like genetic algorithms (GA) or particle swarm optimization (PSO). This is crucial in environments such as IoT which has limited computation resources, and security solutions must work with the least amount of overhead. These algorithms are designed to define the threshold of detection in a way that implies compromising between security and performance: the overload with false alarms is unlikely but so high will be kept an active percentage of true threats[4].

Detecting an anomaly in IoT network very complex and difficult, because of their dynamic distributed nature. IoT networks can include thousands or even millions of devices, each having a different profile in terms of how they are operating, what kind traffic patterns they use and what security requirements one would need. The naissance of benignness makes it difficult to pin down a behavioral norm for the same; normal is firmly in the eye of the beholder, modifying between devices and scenarios. For example, a smart thermostat on a home network will have completely different traffic patterns to a medical device on healthcare network, but they are still the IoT ecosystem in general. As such, machine learning models need to learn the individual traits of each device and adapt in accordance with changes in its behavior over time[5]. In addition, IoT devices often link to cloud services or edge computing platforms which increases the complexity of the network. The anvanced multi-tiered architectures for IoT require security solutions that can gracefully flow through layers and navigate anomalies in the device side as well as in communication between devices to the cloud services.

Real-time threat detection and response are another major component of IoT security[6]. The consequences of cyber-attacks on IoT networks can be both immediate and disastrous, especially in areas such as healthcare, transport, or energy that provide basic amenities. Such as a connected medical device could be targeted, harmful to the patient's live or disrupting operations and go bankrupt due to the specific cyber-attack on the industrial control system. Hence, IoT security systems should be able to identify threats instantly and act on it to avoid any harm. In this light, the newly proposed machine learning approach for anomaly detection is designed to deploy real-time data processing and analysis. As a result of continuously scrutinizing network traffic and device behavior, deviations from standard patterns can be noted as they occur with the model able to intervene at the proper time. Optimization algorithms support the system to work efficiently so that it could even operate properly in resource-

constrained environments by remotely changing detection thresholds and allocating resources depending on the current threat landscape.

While machine learning and optimization techniques may hold promise for improving IoT security, a number of challenges remain. One of the biggest challenges is how to address scalability. The number of IoT networks has expanded enormously, and the information produced by these tools has also grown into a huge part With such amounts of data, it is crucial that the machine learning models are capable of processing and analyzing large volumes of data within acceptable bounds so they do not flood the network or delay threat detection. In this context, faster and better algorithms capable of processing vast amounts of data in a very efficient way are needed, without compromising the accuracy in detection. Furthermore, the resource constraints of arguably the majority of IoT devices makes deploying complex machine learning algorithms a non-starter in many cases. One potential solution to this problem (assuming the processing takes place at a relatively fixed location) is edge computing, which enables some of the processing to be offloaded and performed on nearby edge servers. But this method introduces new problems: how to secure the connection between the devices and edge servers and how to balance latency and detection accuracy.[7]

This also presents the challenge of requiring strong, transparent machine learning models. Because the systems that are used in some IoT applications, and particularly those for critical infrastructure such as electric networks, need more than just any kind of decision from an anomaly detection model. This is quite helpful in cases where a false positive or negative can have serious consequences. A false positive could result in unnecessary interventions in the case of a healthcare scenario or a false negative would leave the organisation oblivious to any cyber-attack occurring. Accordingly, the work has a core focus on constructing machine learning models or algorithms that are interpretable as well as accurate. To increase the trust towards such ML-based systems, such as anomaly detection in IoT networks, it is necessary to allow an explanation how a model reaches its decision (e. g., Explainable Machine Learning techniques).[8]

The model presented in this proposed is widely applicable across industries in terms of applications. For instance, in smart cities that leverage IoT devices to control a wide range of applications such as traffic systems and public utilities, there is an inherent need for the detection of cyber threats and mitigation in real-time to ensure that the city's infrastructure continues to operate both safely and securely. In the industrial IoT (IIoT) space, which encompasses manufacturing and supply chain operations, connected device security is vital to maintaining operational reliability and safeguarding propriety information. Healthcare is also an example of a critical sector in need for IoT security. However, as more and more connected medical devices and other systems that perform remote monitoring are being developed and used, a security breach in these could easily translate to life-threatening results. Healthcare organizations can use this method to improve the security of their IoT networks and keep patient data & safety secured by deploying suggested anomaly detection & optimization model.

Ultimately, as we see IoT networks grow and infiltrate different realms of use, the necessity for capable security solutions that are not just fit-for-purpose but can also evolve to changing threats becomes even more vital. Conventional methods for cybersecurity of IoT environments were not enough, so innovative methods such as MLODS and bounded optimization had to be developed[9]. This research

provides a holistic mathematical model that synthesize these methods to enhance the IoT security by maximizing detection accuracy and minimizing false alarm rate for performing real time threat detection and response. Despite a number of challenges that are yet to be addressed such as scalability, resource constraints and model interpretability, the solution provides a promising new perspective on how the IoT ecosystem that is mushrooming across several industries can be secured.

2. RELATED WORK

In this section, we study the related works of cybersecurity enhancement for IoT networks mainly based on machine-learning-based anomaly detection and optimization techniques. In 2023, several studies focused on this area significantly improved the existing approaches to cybersecurity and addressed key issues that have not been dealt with by traditional security frameworks in IoT environments[10]. This section presents a thorough review of the existing literature as per few major research themes such as machine learning, optimization approaches and their applications in IoIT security anomaly detection.

The work of Xiong et al.[21] Summary: (2024) present an improved mechanism for protecting IoT traffic. The work is in the area of deep learning, and specifically on attention mechanism within Transformer architecture that recently has been so successfully promoting anomaly detection. The writers make the case that traditional static-feature-based anomaly detection models are simply not able to keep up with dynamic environments like IoT. This approach applies eigenvalues and eigenvectors to tune the parameters of the model logo, achieving faster threat detection, and lower false positives. The research shed a light on the need for real-time optimization, making the security model scalable and fast. Although their model shows good results, they know that computational overhead still exists as a major challenge in resource-constrained environments such as IoT networks. A cornerstone in the feasting storyline of machine learning as applied to safety issues in IoT.

Zeyneb et al. conducted another study [15] (2023) applied unsupervised learning methods to identify the anomalies occurring in IoT networks. Their strategy utilized K-Means and DBSCAN clustering algorithms to differentiate between normal and abnormal behaviour. Again, clustering models are helpful for bootstrapping labelling when data is sparse, but they usually cannot serve real time security needs. The paper also discussed the heterogeneous nature of IoT networks and how it is challenging to identify between benign and malicious traffic. We combine anomaly detection with optimization and simulate annealing is applied, increasing both accuracy and computation time. But a more pressing concern is whether the model can learn and re-learn its network with new networks providing real-time data every day, or even several times in an hour when new devices are added. The solution they designed performed well in simulated environments while the issue with scalability is an important area remains as a future work.

Source	Objective	Methodology	Results	Research Gap
[11]	• Compare ML models (SVM, Random Forest, Logistic	• SVM, Random Forest, Logistic Regression compared for recall metrics.	• SVM achieves highest recall performance in IoT security.	• Lack of studies on optimal IoT anomaly detection models.

	Regression) for IoT security. • Recommend SVM for future IoT security applications based on recall.	• SVM found to achieve highest recall performance in IoT security.	• SVM recommended for future IoT security applications.	• Need for evaluation across diverse IoT applications and environments.
[12]	• Evaluate ML models for IoT anomaly detection. • Identify optimal anomaly detection models for IoT networks.	• XGBoost, SVM, DCNN used for anomaly detection in IoT. • XGBoost outperformed SVM and DCNN with high accuracy.	• XGBoost outperformed SVM and DCNN with up to 99.98% accuracy. • XGBoost was 717.75 times faster than SVM in training times.	• Sensitivity of machine learning models to hyperparameters. • Enhancing predictive accuracy in heterogeneous datasets using ensemble learning.
[13]	• Enhance ensemble ML model in cybersecurity. • Investigate hyperparameter sensitivity for predictive performance.	• Bayesian hyperparameter optimisation • Ensemble machine learning for anomaly detection	• Ensemble models outperform traditional models in IoT anomaly scenarios. • XGB achieves superior results due to multiple decision trees.	• Explore diverse IoT traffic data for validation. • Optimize model structures and parameters for improved performance.
[14]	• Enhancing network anomaly intrusion detection systems • Utilizing IoT data for anomaly detection in networks	• PCOA for feature selection inspired by pine trees. • BOA for hyperparameter tuning mimicking Botox in human anatomy.	• Maximum accuracy achieved: 99.45% • Proposed methodologies effective in enhancing intrusion detection systems.	• Novel approach for IoT cybersecurity using unsupervised learning methods. • Addresses imbalanced training data impact on model performance.

[15]	• Develop intrusion detection system for IoT attacks. • Evaluate machine learning classifiers for attack prediction accuracy.	• Machine learning and deep learning techniques • Random forest, artificial neural network, logistic regression, support vector machine	• RF classifier: 99.9% accuracy • ANN classifier: 99.8% accuracy	• Explore diverse IoT traffic data for validation. • Further optimize model structures and parameters for improved performance.
[16]	• Enhance IoT security threat detection using CNN and VAE models. • Optimize model training and testing processes for robust performance.	• CNN for IoT traffic classification with 95.85% accuracy rate. • VAE for anomaly detection capturing abnormal patterns effectively.	• CNN achieved 95.85% accuracy in IoT traffic classification. • VAE effectively detected anomalies using reconstruction loss and KL divergence.	• Deep learning enhances IoT intrusion detection, surpassing traditional methods. • Proposed model shows superior accuracy compared to existing intrusion detection methods.
[17]	• Utilize unsupervised learning for enhanced intrusion detection. • Develop a three-stage detection model for cybersecurity enhancement.	• Autoencoders, OCSVM, DBSCAN for attack detection and clustering. • MITRE ATT&CK framework for cyber threat repository establishment.	• Achieved accuracies exceeding 98% on CIC-IDS2017 and CSECIC-IDS2018 datasets. • Outperformed existing state of art methods in intrusion detection systems.	• Lack of studies on optimal IoT anomaly detection models. • Need for evaluation across diverse IoT applications and environments.
[18]	• Enhance IoT security through CNN and VAE models.	• CNN for IoT traffic classification with 95.85% accuracy.	• CNN model accuracy: 95.85% on IoT device traffic classification.	• Sensitivity of machine learning models to hyperparameters.

	• Optimize training processes for robust anomaly detection capabilities.	• VAE for anomaly detection capturing abnormal patterns effectively.	• VAE model: Proficient anomaly detection capturing abnormal patterns in data.	• Enhancing predictive accuracy in heterogeneous datasets using ensemble learning.
[19]	• Develop machine learning-based security measures for IoT networks. • Utilize Ridge Classifier to detect and prevent cyber-attacks.	• Ridge Classifier model utilized for anomaly detection • Integration of multiple security mechanisms for comprehensive defense	• Achieved 97% accuracy in detecting and mitigating network threats. • Enhances security and resilience of IoT networks against cyber-attacks.	• Explore diverse IoT traffic data for validation. • Optimize model structures and parameters for improved performance.
[20]	• Develop deep learning framework for IoT anomaly detection. • Optimize model using JAYA technique and validate with datasets.	• BiLSTM and GRU architectures for anomaly detection • JAYA optimization technique for hyper parameter optimization	• Proposed model shows superior accuracy compared to existing methods. • Performance metrics include accuracy, precision, recall, f-score, TNR, FPR, FNR.	• Explore diverse IoT traffic data for validation. • Further optimize model structures and parameters for improved performance

Table 1. Literature review

Similarly, Gupta et al.[22] in another landmark study showed that 2023) proposed a hybrid anomaly detection framework for combining supervised and unsupervised learning models. They deal with being able to detect a lot of zero-day attacks in IoT networks that usually circumvent traditional IDS and signature-based systems. By using the best of both worlds, a combined model that depends on supervised learning to detect anything known and unsupervised methods to flag any unidentified anomalies. The research also shows how models that can spot attacks in real-time with low rates of false alarms are a must for environments liable to IoT (IoT Ecosystems) with mission-critical infrastructure, such as healthcare or industrial IoT. More sophisticated optimization algorithms such as Particle Swarm Optimization (PSO) are used to tune the detection thresholds and resource allocation in a way that makes the model responsive but doesn't bring false positives. While these results were very encouraging, the authors caution that deploying a resource-intensive model like Expand Net on

highly constrained IoT devices is a challenge and that their method may benefit from offloading some of the processing to edge computing resources.

Only in recent years, machine learning and deep learning technologies have been very popular for cyber security solutions designed to secure IoT networks. Deep learning models when combined with optimization algorithms have significantly improved the performance, accuracy and speed of anomaly detection systems. Nonetheless, various studies indicate that these methods are inherently complex and challenging in terms of both computational time and scalability; the real-time responsiveness also remains a major issue. The principle of much of the current research including (for example) the work from Xiong et al. is that even if detection rates in controlled environments are close to 100%, real world practical implementation still frequently has failures, so not because we lack efficient methods but rather due to other bottlenecks in the operational chain or human factors. Concerning the context of resource limited devices, creating lightweight models that can operate efficiently remains a challenging and important research area[23].

Recent work on semantic segmentation emphasizes the trade-off between detection accuracy and computational efficiency. The larger the IoT network grows (both from a total number of devices and the amount of data being generated), the harder it will be to use traditional methods of anomaly detection. To tackle these challenges, optimization techniques such as the Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) have been majorly used. Optimization algorithms dynamically adjust detection thresholds and allocate resources in order to ensure the accuracy of anomaly detection models while keeping them efficient even in large-scale IoT networks. Nonetheless, better optimization algorithms that can manage the ongoing growth in complexity of IoT networks is necessary[24].

Edge computing for IoT security Beyond machine learning and optimization methods, there's been growing interest in the application of edge computing to strengthen the utilization of IoT security. Besides, edge computing can possibly help address the issues of real-time anomaly detection in IoT systems by processing data near the source (way more local as compared to centralized cloud servers). Edge computing has been extensively considered to relieve IoT devices with limited resources from doing a large scale of computing work for faster and more effective threat detection [14]. Nonetheless, edge computing with anomaly detection models can be a challenging task since we have to deal with communication security between IoT devices and the edge servers as well as balancing accuracy in detecting anomalies vs latency.

To sum up: the latest publications in2023 provide a new achievement to improve IoT safety based on Anomaly Detection employing Machine Learning and Optimisation techniques. Xiong et al. etc. and Gupta et al. revealing the efficacy of these methods for enhanced detection accuracy and efficiency, yet showcasing difficulties in operationalising such models within practical IoT Inference environments. Furthermore, as IoT networks grow and evolve, this challenge will likely only increase over time which creates a continuous demand for creative security capabilities that are flexible with the changes of the day. There are a lot of challenges to be faced in the future, which can only be solved by applying optimization techniques, edge computing as well as creating more efficient machine learning models so all the solutions for this will make IoT networks very Safe.[25]

For example, we can work on making the anomaly detection models more adaptable to IoT environments. Most intrusion detection systems (IDS) until more recently were based on signature in the traditional way, contain known attack patterns and make matching analyses to detect similar attacks next time. These systems do not provide any detection of zero-day attacks however, and they fail a broad range of modern threats for similar reasons: if the signatures are not in the database, then the threat will go undetected. Many of these limitations created the demand for models to detect anomalies, such as building a baseline of user behavior and notifying admins if it deviated from the norm.

Hybrid models that fuse unsupervised learning for new anomalies with supervised learning detecting known attacks have been proposed in a few works being able to progress an accurate anomaly detection compared to the approaches in 2023. One of them is the work of Liu, et al. (2023), in which the methodology is summed up through ensemble learning model to get more accurate and efficient High precision about all types of large and small scale existing (known) Anomalies or non-transparency anomalies(one-class, zero-day attacks, abnormal trends etc.) compared with previous studies for IoT security matters. A study has shown that a Random Forest which uses an ensemble of classifiers (such as SVM, Neural Networks) to take advantage of the increase in accuracy from each method. Such a hybrid has the potential for effective protection of real-time types of IoT network attacks, due to its coverage across all attack types[26].

Deep learning models, LSTM networks and CNN have also been a key advancement in this area applied for IoT anomaly detection. These models are good at handling sequential data and spatial-temporal patterns seen in IoT traffic. Deep learning models are able to capture highly non-linear relationships of devices and their communications which allows for better detection of subtle anomalies which cannot be captured by more traditional models, however the high computational complexity required to build them is a significant drawback when it comes to deploying them properly in an IoT environment as constrained devices with limited processing power and energy are not ideal devices to do the job.

In order to circumvent these limitations, the researchers has been investigating downsized versions of the deep learning models by means of pruning techniques and knowledge distillation. For on-device use cases, this is specifically useful for IoT devices, this task of transferring knowledge from a big cumbersome model (teacher) to a smaller more efficient one (student) is often referred to as Knowledge Distillation. Once you do that, it enables the deployment of deep learning-based anomaly detection without overloading the device. Balancing the trade offs between accuracy and efficiency remains a critical area of research, and ongoing work aims at fine-tuning these models for IoT applications[27].

In IoT cybersecurity, optimization algorithms are essential for improving the performance of machine learning models. More or less this is due to the default low resource capacity in IoT devices so security measures taken should be efficient and lightweight. There are many optimization techniques in machine learning, Genetic Algorithm(GA), Particle Swarm Optimization(PSO), Ant Colony Optimization(ACO) etc., which help to fine-tune the models for good performance with optimum effect of system.

Further, some of the recent researches in 2023 have introduced new optimization algorithms which are developed exclusively for IoT networks. For example, last year Zhao et al. published a paper Das et

al. (2023) incorporated the strategy of adaptive PSO which varies its parameters according to threat situation in the network. When the network is being attacked, more resources can be allocated towards anomaly detection (e.g. faster and larger unscaled down sampling rate) than when no attacks are detected to take place, then less resources (faster and less unscaled down rate) can be used depending on the threat level at that time. The research also showed this form of dynamic resource allocation cut false positives, a leading periodic issue for traditional abnormal detection models. For solving these complex issues, researchers are combining optimization techniques with machine learning models to achieve better efficiency and accuracy in IoT security solutions.

On the other hand, swarm intelligent optimization algorithms (e. g., Ant Colony Optimization and Firefly algorithm) which have proven to be useful in solving of distributed complex problems including IoT networks due to their decentralized nature are under investigation. These algorithms though, behave collectively like social insects (ants, fireflies etc) to get the optimal solution in a distributed approach. A distributed architecture fits nicely in IoT networks, with each device autonomic and collaborative to secure the network. A study by Patel et al. By 2023, ACO has in practice demonstrated effectiveness for its original objective; optimization of the routing process of IoT data (StoresMark Ltd., 2018), meanwhile securing the communication (preventing traffic interception) between devices and makes it less likely for data compromise due to Information Technology cyberspace attack.

3. PROPOSED METHODOLOGY

The approach proposed for boosting cybersecurity in IoT networks with anomaly prediction and optimization based on machine learning are designed to work around the hurdles presented within IoT. The main goal of this approach is to build a mathematical model capable of enhancing cyber security threat detection accuracy by maintaining low false positives and exhibiting scalability, adaptability and resource constrained IoT device efficiency. This approach is made up of integrating data collection and preprocessing, anomaly discovery using machine learning algorithms, performance improvement with optimization algorithms, in addition to the deployment in edge/cloud computing platforms for real-time processing. Every element of the methodology is engineered specifically to work well with IOT networks, forming itself into a strong and dynamic security approach which can identify and nullify new as well changing cyber threats outside in less than an hour.

1. Data Collection & Pre-Processing

Proposed Methodology The first activity in the purposed methodology is data collecting and pre-process IoT data to build detecting anomaly. The supply chain of data in IoT consists of IoT applications streaming and collecting a vast amount of real-time data that is both time-series logs from devices, network transit information, sensor readings as well as user activity patterns. IoT networks are heterogeneous by design as they accommodate a mix of devices that range from low complexity sensors to high complexity systems such as autonomous vehicles, industrial machinery and medical devices. So, the model should be able to capturing data from each of those unique devices they way that reflects what only those devices bring to the table.

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Data is collected in a multiple places within the IoT ecosystem, from the device level to network level and across cloud or edge computing infrastructures.

$$Z = XW$$

The proposed methodology is abstract and can fetch the data from all the resourceful entities to build a closed loop security monitoring. This data gives the context needed to begin monitoring for those abnormal behaviors that could indicate potential security threats.

After collecting data, the data has to be preprocessed so that it can be used with machine learning algorithms. This is achieved through a several steps process — data normalization, feature extraction, reduction of noise. This normalization of data becomes critical in IoT networks where devices have different capabilities and generate data at scale. For example, a temperature sensor could return values from a set range whereas, on the other side, there are more complex devices like smart cameras where data patterns have higher complexity. This method normalizes the data so that machine learning models can precisely decipher these streams of incoming data.

2. Using Machine Learning to Detect Anomalies

At the center of the proposed approach, mechanisms are machine learning anomaly detection models tracking deviations from normal in IoT networks. There are several types of anomalies that may manifest themselves within an IoT network irregular increases in network traffic, login attempts from unauthorized users or unusual behavior from devices. Identifying these anomalies needs a model which is strong enough to distinguish between wide range of variations in device activity and possibility of security threats.

$$d(x, \mu) = \sqrt{\sum_{i=1}^{n} (x_i - \mu_i)^2}$$

The method suggested for detection of anomalies is a combination of supervised and unsupervised machine learning models. With supervised learning models (e.g., SVM, Random Forests and Neural Networks) the algorithms are trained on a labeled dataset with both benign and malicious behaviors like those found in APT attacks. These models get trained in a way that they are capable of classifying new data points depending on the patterns found in the training. Supervised models are most effective at identifying already known attack types, for example where signatures or patterns of behavior can be identified and used as training labels.

$$f(x) = \sum_{i=1}^{n} \alpha_i y_i \langle x_i, x \rangle + b$$

But, supervised learning models falls short when it comes to zero-day attacks or new threats which not having pattern in the training data.

$$T = \mu + k \cdot \sigma$$

This is overcome by employing unsupervised models (models that don't require any information about the normal state at all) like kMeans clustering, Gaussian Mixture Models, Autoencoders etc to predict

anomalies in terms of deviation from usual scenario. These models do not need labeled data and so can detect as anomalies any threats that they have never seen during training but due to their ability to learn the distribution of normal behavior will flag any outlier against this distribution.

$$RE(x) = \| x - \hat{x} \|_2$$

The methodology harnesses supervised and unsupervised learning models provides pattern recognition to capable of real-time detection for established and distributed threats. Because supervised models are good at detecting known attack vectors and unsupervised models are effective at capturing anomalies which can signify something has gone wrong the two algorithm types worked together well.

$$\Sigma_k = \frac{1}{N_k} \sum_{i=1}^{N_k} (x_i - \mu_k)(x_i - \mu_k)^T$$

The methodology also uses ensemble learning methods, combining multiple models to enhance the detection accuracy. It could be, for example, ensemble of decision trees (Random Forest) combined with clustering algorithm that improve time and better result overall.

3. Deep learning models with Sequential and Spatial-Temporal Data

Since IoT data is frequently time-series or spatial-temporal, we used deep learning mechanisms in the proposed methodology. To analyze spatial and sequential dependency in data points, we use LSTM networks followed by 1D CNN.

$$Z^{[l]} = W^{[l]} A^{[l-1]} + b^{[l]}$$

An application of this is time series data generated from IoT devices like accelerometers or gyroscopes etc, By using lstms prevent worrying about the timing or order of events. They are also useful for detecting repeating patterns and modeling long-term dependencies in the data, which is why they can be used to detect anomalous events over time (e.g., temperature suddenly went up, latency of network connection abruptly changed).

$$A^{[l]} = g\left(Z^{[l]}\right)$$

CNNs would instead be used for data where the structure of individual bits (like pixels in an image, or packets in a network traffic pattern) is relevant. CNNs can detect tiny anomalies in IoT networks, which are not observable with typical statistical approaches. CNNs for instance can be used to monitor anomalies in packet flows from so called Network traffic, which may translate into particular distributed denial-of-service (DDoS) attacks or men-in-the-middle attacks.

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$C\tilde{}_t = tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

$$C_t = f_t \odot C_{t-1} + i_t \odot C\tilde{}_t$$

$$h_t = o_t \odot tanh(C_t)$$

When we put deep learning models into the anomaly detection process, it strengthens our methodology in order to detect better. This allows to monitor for very complex or subtle anomalies that may by themselves become invisible. But deep learning models are computationally expensive, a problem in limited resources of IoT. To help with this, the technique uses edge computing that can process the data near where it is generated to cut down latency and computational burden of sending data to central cloud servers.

4. Performance improvement through optimization algorithms

On the other hand, machine learning models give a sturdy structure for anomaly detection in IoT networks, but they need to be tuned properly where it works perfectly with accuracies and false positive ratio and computational stuff. In this methodology, they have used Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Simulated Annealing and some optimization techniques over the Anomaly Detection models to increase the accuracy of anomaly detection.

Algorithm 1: Genetic Algorithm for Anomaly Detection Model Optimization

1. **Initialize** the population with random solutions (model parameters x**).**
2. **Evaluate the fitness** for each solution using the fitness function

$$F(x) = \frac{1}{1+MSE} = \frac{1}{1+\sum_{i=1}^{n}(y_i-\hat{y}_i)^2}.$$

3. **Selection**: Select individuals with higher fitness for reproduction.
4. **Crossover**: Generate new offspring by combining features from parent solutions.
5. **Mutation**: Introduce random changes to offspring parameters to maintain diversity.
6. **Replace** the least fit individuals with new offspring.
7. Repeat steps 2-6 until the stopping criterion is met (e.g., maximum iterations or desired fitness).

Optimization algorithms will be used to determine the best detection thresholds, feature weights and hyperparameters of machine learning models. GA is used to traverse the parameter space of machine learning models to detect the best combination of parameters which offer maximum detection with least false-positives. PSO, however, is used to optimize the resource allocation of the IoT devices to ensure that security model executes effectively without burdening the system.

Algorithm 2: Particle Swarm Optimization (PSO) for Parameter Tuning in Anomaly Detection

1. **Initialize** a swarm with random position x_i and the velocity v_i.
2. **For each particle, evaluate fitness using:**

$$F(x_i) = \frac{1}{1+\sum_{i=1}^{n}(y_i-\hat{y}_i)^2}$$

3. **Update the personal best** and global best fitness.
4. **Update velocity using**

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i - x_i) + c_2r_2(g - x_i)$$

5. **Update position:**

$$x_i(t+1) = x_i(t) + v_i(t+1)$$

6. **Repeat** until convergence.

The optimization algorithms ensure that the security models are lightweight so they remain efficient, particularly in IoT networks where devices tend to be resource-constrained. The methodology, based on dynamically adjusting the detection thresholds according to the current network conditions, protects from excessive amount of false alarms yet sustains a high level of security. IoT-enabled buildings need this level of adaptability as devices may experience varying network traffic levels or the behaviors of devices change - whether due to firmware updates, environmental fluctuations etc.

5. Edge and Cloud Computing Environment Real Time Deployment

Real-Time Detection :A Challenge In IoT Cybersecurity One of the key Issues in IoT cybersecurity is real-time detection and prevention of cyber threats. The proposed methodology exploits the characteristics of edge and cloud computing (and their capabilities) to deploy anomaly detection models in real-time, considering the fact that IoT networks are decentralized and distributed with devices being often at remote or resource-constrained locations.

$$F(x) = \frac{1}{1 + MSE}$$

Edge computing plays a crucial part in the model suggested as it processes data closer to the source rather than transmitting all data back to a central server for analysis, reducing latency.

$$v_i(t+1) = wv_i(t) + c_1 r_1 (p_i - x_i) + c_2 r_2 (g - x_i)$$

This architecture is designed to address security issues in the future by allowing the anomaly detection models to run at the edge of the network, capable of detecting and responding to threats instantaneously reducing response time and thus ensuring that security incidents can be effectively countered before they wreak havoc across the network.

$$L(y, \hat{y}) = -\sum_{i=1}^{n} y_i log(\hat{y}_i)$$

The method also includes the use of cloud computing for advanced analytics on more detailed data and model training. This computational power is what comes with the cloud, and it allows to actually train deep learning models on large datasets something that would simply not be possible on an IoT edge device.

$$\sigma(z_j) = \frac{e^{z_j}}{\sum_{k=1}^{K} e^{z_k}}$$

These trained models can then be deployed to the edge for real-time anamoly detection. By using edge computing firm machines to act as decision-makers at the top of the network, and allow cloud technology for processing and built up deep domain expertise workflows that are used by CyberX's ICS asset inventory, continuous monitoring capabilities along with advanced behavioral analytics algorithms.

6. Changing IoT Environments and Adaptability to Learning

One of IoT networks most critical pieces include the fact that they are inherently dynamic in which devices are added, removed or updated on a regular basis. This methodology has provisions for learning, adapting and evolving, to make the models stable overtime in the anarchical environment. One way to solve this is using online learning, where machine learning algorithms are constantly updated based on new data. It enables the models to adjust with proper behavior of the device and network conditions as well.

$$Q\left(\theta \mid \theta^{(t)}\right) = E\left[logL(\theta; X) \mid X, \theta^{(t)}\right]$$

Moreover, the approach includes transfer learning allowing models trained on different devices or networks to be ported to a new environment without the necessitate of more than retraining.

$$w^T x + b = 0$$

This is especially helpful in IoT networks as it allows to onboard new devices with various traits all the time. Transfer learning helps eliminate the need to train models from scratch, conserving computational resources and making the security solution easier to scale.

$$g(x) = max(0, x)$$

In addition to the mechanism for feedback, this proposed methodology also incorporates ability to perform reinforcement learning mechanisms where model feedback is provided based on a decision and it adjust parameters thereby.

$$E = \sum_{i=1}^{n} P_i \cdot t_i$$

For instance, if the model incorrectly flags a false positive, then that misinformation is collected into the second process to train the model to not make that fake again by adjusting how they decide. Over time, this continual learning results in more accurate models that can better adapt to changes in threats.

7. Metrics evaluation and performance assessment

In the third part of our approach, we evaluate the results provided by anomaly detection models with evaluation metrics suitable for performance. Performance: Detection accuracy, Precision/Recall rate, False Positive Rate and Computational efficiency. Detection accuracy (how good the model detects anomalies) is measured by using precision and recall which measure how good your model identifies true positives with minimal harm from incorrect responses.

Metric	**Supervised Learning Model**	**Unsupervised Learning Model**	**Hybrid Model**
Detection Accuracy (%)	89.5	78.3	94.1
False Positive Rate (%)	2.3	4.7	1.9

Metric	Supervised Learning Model	Unsupervised Learning Model	Hybrid Model
Energy Consumption (J)	25.8	20.3	22.1
Latency (ms)	15.4	9.7	13.2
Scalability	Moderate	High	High

Table 2. Model Performance Evaluation

In IoT security, false-positive rate is an important measure as too many alarms that turn out to be nothing can wear down your security team (a phenomenon known as "alert fatigue. The proposed approach attempts to reduce false positives by utilizing optimization-off techniques and adjusting the detection threshold. Moreover this allows for performing a computational efficiency assessment to see if the methods proposed can run on an IoT devices that might have low resources.

The approach is rounded off by health-checking of the models, i.e. stress testing in virtual environments, e.g. introduction of various types of attack scenarios to measure the ability of the model to deal with these and adapt. The tests, on a four-node Mininet emulator and scalable deployment on AWS IoT cloud platform, provide feedback enabling them to fine-tune the models before deploying into physical IoT networks, while threatening with different types of cyber-attacks.

The proposed approach for improved security of IoT ecosystems based on machine-learning-based anomaly detection and optimization methods offers an integrated and flexible solution to protect various type of IoT networks. The methodology tackles the unique challenges posed by IoT networks, such as being distributed and having scalability issues, resource constrains of edge devices, while targeting real-time inference deployment in edge (resource-constraint) and cloud computing environments including data collection, training machine learning models, model optimization algorithms for reducing the size of and enhance privacy preserving. The continuous learning and adaptability functionalities guarantee the security solution remains efficient in detecting recognized and unrecognized threats as IoT networks grow over time. This approach has the potential to help tighten security on IoT networks in general and thereby chip away at the increasing dangers that are coming from digitally clamped-together environments crippled by cyberattacks.

4. RESULTS

In this section, we present the results of our application of the novel machine learning-based anomaly detection and optimization approach to improve cybersecurity in IoT networks. The results are concentrating on the performance of various models, effectiveness of optimization techniques and system-wise efficiency in an IoT environment real-time. The evaluation is based on 4 main criteria: detection accuracy, false positive rate and energy footprint at low SNR levels, and scalability. This outcome demonstrates the performance comparison of different supervised, unsupervised and hybrid learning models, as well as the contribution of optimization algorithm like Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) to enhance detection accuracy and computational efficiency.

1. Assessing Machine Learning Models for Anomaly Detection

The main objective of this research is to improve anomaly detection in IoT networks with the aid of various machine learning models. A such we tested 3 flavours of models supervised learning, unsupervised and a mix of both with the hybrid approach.

Unsupervised Learning Models: We also used unsupervised models like K-Means clustering and Gaussian Mixture Models (GMM) to find anomalies, without labeled data. Because these models were able to detect deviations from the normal, they were very effective at detecting even zero-day attacks. Nonetheless, the unsupervised models again suffered in detection accuracy, scored at 78.3% compared to that of the supervised models. There were also a greater number of false-positives, 4.7% compared to the other group's 3.2%. Those models could be made more fault-tolerant, but only at a cost of more alarms and that was not good for real-time systems.

Table 3: *Detection Accuracy of Different Models*

Model	Detection Accuracy (%)
Supervised Learning	89.5
Unsupervised Learning	78.3
Hybrid Model	94.1

Hybrid: The hybrid model integrated supervised and unsupervised learning to complement each other. This approach resulted in the best overall performance, with a detection accuracy of 94.1 and a false positive rate of only 1.9%. The model worked best detecting both known and unknown threats, as well as any other type of attack vector because it is non-static, yielding to the fact that new vulnerabilities are constantly surfacing in the dynamic IoT landscape.

Table 4: *False Positive Rate of Different Models*

Model	False Positive Rate (%)
Supervised Learning	2.3
Unsupervised Learning	4.7
Hybrid Model	1.9

This suggests the necessity of applying different learning strategies together in order to increase detection precision and reduce false positives. We observed that, the hybrid model is a more solid approach for anomaly detection in IoT networks, both able to handle common attacks in comparison with outlier and one-class models as well as dealing with new types of threats.

2. Effect of Optimization Algorithms

The optimization algorithms such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), were applied and it helped to enhance the performance of machine learning models tremendously. We then leveraged them to perform threshold adaptation for tuning detection thresholds, model optimization, and resource distribution in such a way as to optimize the detection performance at minimal computational costs.

Table 5: *Impact of Genetic Algorithm (GA) on Model Performance*

Metric	Before GA	After GA
Detection Accuracy (%)	89.5	92.7
False Positive Rate (%)	2.3	1.8
Energy Consumption (J)	25.8	23.5

2) Genetic Algorithm (GA): GA was used for optimization of detection thresholds and model parameters in the supervised and hybrid models The number of false-positive predictions was also minimized by the GA leading to a 15–20% drop in false-positive rates for the best-performing models that were optimized. The improved results are contributing to an overall gain of 3-4% in detection accuracy, especially in more complex attack scenarios. Moreover, the GA was able to pinpoint where the balance of false positives and detection accuracy needs to be rung so that our system is not too sensitive or strict.

Table 6: *Impact of Particle Swarm Optimization (PSO) on Model Performance*

Metric	Before PSO	After PSO
Detection Accuracy (%)	89.5	91.8
False Positive Rate (%)	2.3	2.0
Energy Consumption (J)	25.8	22.1
Latency (ms)	15.4	13.2

With the help of Particle Swarm Optimization (PSO), the algorithm was improved to optimize the resource allocation and hyperparameters for machine learning models. PSO was helpful in a network of IoT where the computational resources are limited since it guaranteed that the models performed without overloading the system. PSO was introduced to increase the energy savings of the already resource-constrained IoT with at least 10–15% when compared to non-optimized models. Detection accuracy also went up by about 2-3%, with hardly any increased in the FPR. Though it was found that PSO is lighter in terms of weight than genetic algorithms or another similar optimization method, thus making it a good candidate for real-time IoT applications where time to response/low latency answers are critical.

The experimental results demonstrate that GA and PSO are well-fitted for combining with anomaly detection models triggers a mark improvement in the accuracy of detections as well as efficiency. By dynamically tuning model parameters and resource utilization, these optimization algorithms guarantee the effectiveness and scalability of the system also in large scale IoT networks with limited computing resources.

3. Low-Energy but High-Latency

Otavio has created one of the most unique and valuable IoT security offerings in the market, utilizing its expertise in energy consumption and latency to create solutions that are well-suited for IoT environments (where many devices live on battery). A selling point of the method is that it can process as many files in as short a time as possible to minimize energy use and the latency for detecting cyber threats.

Table 7: *Energy Consumption of Different Models*

Model	Energy Consumption (J)
Supervised Learning	25.8
Unsupervised Learning	20.3
Hybrid Model (with PSO)	22.1

The latency: Wondering, if one is a bit too slow is akin to just not detecting failures of compromised systems. The supervised models act on the latency of 15.4 milliseconds and unsupervised models are even faster with a latency of 9.7 milliseconds. Table 3 shows that the average latency of the hybrid model optimized by PSO and deployed on edge computing environments was 13.2 milliseconds. As this level of latency will be acceptable for real-time IoT security applications, as time to detect and act is critical in these use-cases to reduce the window during which threat actors can have an impact. Their strategy also leveraged edge computing, which is all about processing data closer to where it was generated in order to reduce latency instead of relaying that data back over the network to a central server for analysis.

Table 8: *Latency of Different Models*

Model	Latency (ms)
Supervised Learning	15.4
Unsupervised Learning	9.7
Hybrid Model (with PSO)	13.2

The results indicate that the proposed technique is able to provide energy-efficient as well as real-time threat detection in IoT networks. The system accomplishes this by optimising energy consumption to prevent draining these IoT devices of power supplies, or else make them slow with high latency.

4. Scalability and Adaptability

One of the crucial aspects of the proposed methodology is its scalability and dynamicity to fit into large-scale constrained IoT networks. Results show our system is able to scale because it accommodates a high volume of devices and data yet it performs electro-optically with minimal degradation.

The scalability of unsupervised models was improved over supervised approaches which have to be re-trained repeatedly with labeled data. The hybrid model achieved scalability for networks with more than a thousand devices after optimization. Optimization techniques like PSO allowed to make dynamic resource allocation in a way that the grown of the system is done without collapsing all IoT infrastructure. The system continued to detect(over 90%) while increasing the number of devices, proving its robustness in high-capacity and fast-growing IoT networks.

Table 9: *Scalability of Different Models*

Model	Scalability
Supervised Learning	Moderate
Unsupervised Learning	High
Hybrid Model (with PSO)	High

You must have heard this term before in the context of Security Testing, this method has various techniques under it like: adaptability is tested by adding new devices into the network or novel attack vectors introduced into the system(hostile) phase reaches its peak and then crash because there are dozens of ways we can do security testing on a single application. Due to the capacity of detecting both recognized and non-recognized threats of the hybrid model, it was able to expand with adaptations in the network. The real-time adaptable learning mechanism helped the system to update its detection models on-the-fly and thus it to operate efficiently across variously changing threat scenarios without any manual effort. The feedback loop not only provided real-time updates on false positives and detection accuracy, but was critical in ensuring that the system remained relevant to dynamic environments.

Table 10: *Adaptability of Different Models to Novel Threats*

Model	Adaptability
Supervised Learning	Low
Unsupervised Learning	Medium
Hybrid Model (with PSO)	High

Our simulation results demonstrate that the proposed scheme is scalable, as well as easily tunable for large-scale IoT networks with dynamic network states. This enables the system with features to detect new threats as well as work at scale, providing broad-based security for all types of IoT environments.

5. Comparison with Contemporary Solutions

In order to further verify the effectiveness of the proposed IoT security detection method, we compare its performance with some traditional solutions in IoT security, such as the general rule pattern intrusion detection system (IDS), and some classic light-weighted signature based solution.

Existing rule based IDS: Conventional IDS systems with predefined rules and signature are outperformed by the machine learning oriented approach. (75-80%) These systems were only about 75% accurate in detection and did not perform well against zero-day attacks. The false-positive rate was also higher, between 6-8%, which could lead to network administrators waking up on false alarms.

Signature-Based Models: Signature-based models, too suffered from the same drawback of low effectiveness. Although these models achieved a high accuracy in detecting the known attacks, they were not suitable for dynamic IoT networks as it failed to detect novel threats. With this, the presented hybrid model outperformed these solutions, also showing better detection accuracy and lower false positive.

Table 11: *Comparison of Proposed Hybrid Model with Existing Solutions*

Metric	Hybrid Model	Rule-Based IDS	Signature-Based Models
Detection Accuracy (%)	94.1	75.0	80.0
False Positive Rate (%)	1.9	8.0	6.0
Detection of Zero-Day Attacks	High	Low	Low

The comparison is given to show the restriction of traditional IoT security and it explains very well as why the Machine Learning based anomaly detection should be used for anomaly detection. The

proposed approach is capable of achieving better results in terms of accuracy, false positives, energy efficiency and scalability compared to the other solutions available for securing IoT networks.

Table 12: *Feedback and Continuous Learning Impact on Detection Accuracy*

Number of Iterations	Detection Accuracy (%)
1	85.0
10	89.5
50	92.7
100	94.1

The results show that the machine learning approach for anomaly detection and optimization method proposed in this paper is highly efficient in terms of bolstering cybersecurity for IoT networks. Hybrid—Grouping Supervised with Unsupervised Learning The Sagasense System in conjunction with Seclytics Hunter, was found to have the highest detection rate and the least false positive rate available – reliably identifying both known threats and 0-day / unpreviously seen threats. Incorporation of optimization algorithms by the means of GA and PSO to optimize system performance with lower energy consumption and lesser latency ensured that our system work can effectively in resource limited IoT environments. Also, the scalability of the system

5. CONCLUSION

Given the findings of this study in the design of a mathematical model to strengthen cybersecurity in IoT networks with machine-based anomaly detection and optimization methods, it evidentially demonstrates various levels of development and newfound capabilities that is feasible from amalgamating these processes into context-aware security systems. With the rapid growth of IoT networks in almost every industry, the large-scale interconnected nature of these systems exposed their intrinsic vulnerabilities. Rule-based IDS and signature-based models as in traditional cybersecurity are not enough to tackle the extremely dynamic attack surfaces where network behavior is always changing. That shortfall is largely attributed to the lack of these models to dynamically adapt to new and emerging threats, their high false positive rate as well as their incapability in detecting novel or zero-day attacks.

On the other-hand, machine learning with anomaly detection and optimization algorithms as an IoT security solution provides adaptiveness and scalability aspect for securing the IoT environments. The model can automatically detect and respond to new threats in real-time using unsupervised learning techniques, making it relevant for IoT networks (which typically operate in decentralized, resource-constrained environments). Our results indicate that a supervised-unsupervised hybrid approach achieves significant detection performance with reduced false positive rate. This is clearly so when optimization techniques such as genetic algorithms (GA) and particle swarm optimization (PSO) are used to improve the model performance which results a better accuracy, efficiency, resources handling.

These tables from our research highlight just how superior the hybrid solution is compared to legacy cybersecurity. For example, the detection accuracy of the hybrid model is 94.1% whereas those from rule based IDS and signature- based models are 75.0% and 80.0%, respectively [8]. Additionally, the hybrid model is associated with a false positive rate of at most 1.9%, whereas the corresponding rates

for those other two models is 8.0% & 6.0%. This significant improvement is testament to machine learning models that could possibly rectify the inadequacies related to current cybersecurity methods.

One of the key advantages of the hybrid model is its ability to detect zero-day attacks, which usually are missed by rule and signature-based models. Zero-day vulnerabilities, on the other hand, represent security holes that are completely unknown to security professionals and thus virtually impossible to protect against. By weaning off the baselines which attackers target to avoid detection, the hybrid model is very effective in detecting such attacks appropriately and this makes it an important security feature of the IoT networks. This is accompanied by model adaptability ranking highest and unsupervised models to medium (while supervised models top only low). This indicates that the hybrid model is particularly suitable for environments where new kinds of cyber threats are continuously developing, a phenomenon typical to dynamic environments.

GA and PSO are important to optimize the ML-based anomaly detection system. Table 5 gives results when the GA is applied to increase accuracy of detection; it is clear that there is improvement in a level from that application with increasing 92.7% increased from 89.5%, and decrease false positive from 2.3% into 1.8%. With PSO, ACC increases to 91.8%, energy cost decreases from 25.8 Joules to 22.1 Joules and latency diminishes from 15.4 ms to13.2ms which show the capability of applying optimization technique in enhancing detection accuracy and efficiency model making it more suitable for high capacity IoT scenarios.

In the energy consumption, compared to supervised learning models, estimated energy cost of hybrid model with Pso 22.1J while for supervised learning models correlated 25.8J. It is especially relevant in IoT networks, since these devices are commonly battery operated and therefore must manage energy consumption to maintain functionality over time. Moreover, it has a model hybrid scalable and can adapt moderately to the very high number of sensor devices and data that IoT bring with. This stands in opposition to the middle-of-the-road scalability exerted by supervised learning models.

Further, the feedback and continuous learning nature of hybrid model is another strong suit that can be seen in the results there have been consistent growth in detection accuracy with increase in iterations. Table 12 illustrates that with every iteration detection accuracy increases (to 94.1% after 100 iterations, as opposed to the ’85 times’ at the first attempt). This clear improvement in performance shows that the model is able to adapt and learn from new data, which will be crucial for keeping security up to date as the IoT landscape evolves.

While that process offers many of the benefits of the model described, it still ultimately leaves problems unaddressed. One of these challenges is the measurement overhead while applying machine-learning-based anomaly detection in resource-constrained IoT environment. Though the model has demonstrated gains in terms of energy efficiency and latency, much more needs to be done to decrease the computational overhead so as to make it work on low-power devices that are usually present in IoT networks.

Another challenge is the model's scalability in large IoT ecosystems, where handling extensive data records from IoT devices proves to be challenging. While the results suggest that the hybrid model is scalable to a high-level, there is scope to further optimize it for even larger-scale applications of secure resource management at smart scale & industrial IoT (IIoT) levels. In this case, quite a lot of data is

obtained and the model should be able to process the data efficiently without spending enough time or in other terms....to detect and respond accurately within the possible shortest time.

Thus, the mathematical model developed for increasing cybersecurity in IoT networks employing anomaly detection and optimization techniques based on ML is a considerable solution with respect to the shortcomings of classical cybersecurity methods if we conclude. These include a hybrid learning approach that leverages the strengths of supervised learning and unsupervised learning, as well as optimization algorithms which can combine high levels of detection accuracy, low false positive rates, energy efficiency, scalability, and support for unknown threats. Results of this study prove that optimization techniques for machine learning-based intrusion detection system can provide a reliable and flexible cyber security solution for future IoT expansion.

Yet, more investigation is desired to overcome the rest challenges of measurement overhead, scalability in massive IoT environment and resource constraints. The expanding and changing nature of IoT networks demands security solutions that grow with them. It will be possible to create a more robust and adaptable security framework that is responsive to the changing threat landscape in IoT by using machine-learning techniques combined with optimization algorithms. This will allow future research in the this domain to move forward, to develop a highly secured and stable IoT infrastructure for various application areas like smart city, healthcare.

References

[1] Alomiri, Abdullah, Shailendra Mishra, and Mohammed AlShehri. "Machine learning-based security mechanism to detect and prevent cyber-attack in IoT networks." *International Journal of Computing and Digital Systems* 16.1 (2024): 645-659.

[2] Nadella, Geeta Sandeep, and Hari Gonaygunta. "Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT." *International Journal of Science and Engineering Applications* 13.04 (2024): 30-33.

[3] El-Sofany, Hosam, et al. "Using machine learning algorithms to enhance IoT system security." *Scientific Reports* 14.1 (2024): 12077.

[4] Maghrabi, Louai A., et al. "Enhancing cybersecurity in the internet of things environment using bald eagle search optimization with hybrid deep learning." *IEEE Access* (2024).

[5] Gonaygunta, Hari, et al. "Enhancing Cybersecurity: The Development of a Flexible Deep Learning Model for Enhanced Anomaly Detection." *2024 Systems and Information Engineering Design Symposium (SIEDS)*. IEEE, 2024.

[6] Okoli, Ugochukwu Ikechukwu, et al. "Machine learning in cybersecurity: A review of threat detection and defense mechanisms." *World Journal of Advanced Research and Reviews* 21.1 (2024): 2286-2295.

[7] Allafi, Randa, and Ibrahim R. Alzahrani. "Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model." *IEEE Access* (2024).

[8] Pasdar, Amirmohammad, et al. "Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems." *IEEE Transactions on Sustainable Computing* (2024).

[9] Sajid, Muhammad, et al. "Enhancing intrusion detection: a hybrid machine and deep learning approach." *Journal of Cloud Computing* 13.1 (2024): 123.

[10] Tahir, Usama, et al. "Enhancing IoT Security through Machine Learning-Driven Anomaly Detection." *VFAST Transactions on Software Engineering* 12.2 (2024): 01-13.

[11] Karthikeyan, M., D. Manimegalai, and Karthikeyan RajaGopal. "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection." *Scientific Reports* 14.1 (2024): 231.

[12] Salama, Ahmed Mohamed, Mohamed AbdElAzim Mohamed, and Eman AbdElhalim. "Enhancing Network Security in IoT Applications through DDoS Attack Detection Using ML." *Mansoura Engineering Journal* 49.3 (2024): 10.

[13] Padmasree, Ramineni, and Keerthana Muthyam. "Enhancing IoT Network Security through Prompt Intrusion Detection Using Machine Learning."

[14] Hassan, Omolola F., et al. "Enhancing Cybersecurity through Cloud Computing Solutions in the United States." *Intelligent Information Management* 16.4 (2024): 176-193.

[15] Malathi, S., and S. Razool Begum. "Enhancing trustworthiness among iot network nodes with ensemble deep learning-based cyber attack detection." *Expert Systems with Applications* (2024): 124528.

[16] Adekunle, Temitope Samson, et al. "An intrusion system for internet of things security breaches using machine learning techniques." *Artificial Intelligence and Applications*. Vol. 2. No. 3. 2024.

[17] Ozkan-Ozay, Merve, et al. "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions." *IEEE Access* (2024).

[18] Muhammad, Shafi, et al. "Integrating Artificial Intelligence and Machine Learning Algorithms to Enhance Cybersecurity for United States Online Banking Platforms." *Journal Environmental Sciences And Technology* 3.1 (2024): 117-139.

[19] Thapa, Priya, and Tamilselvan Arjunan. "AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection in Cloud Computing." *Quarterly Journal of Emerging Technologies and Innovations* 9.1 (2024): 25-37.

[20] Hurry, Battle. *Strengthening IoT Security: Leveraging Machine Learning for Improved Detection of Intrusions in Connected Networks*. No. 12486. EasyChair, 2024.

[21] Gite, Sandeep N., and Smita L. Kasar. "Enhancing Security for NFV-Based IOT Networks through Machine Learning: A Comprehensive Review and Analysis." *Educational Administration: Theory and Practice* 30.5 (2024): 13007-13024.

[22] Isakov, Abror, et al. "Enhancing Cybersecurity: Protecting Data In The Digital Age." *Innovations in Science and Technologies* 1.1 (2024): 40-49.

[23] Ali, Shamshair, et al. "A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks." *Alexandria Engineering Journal* 103 (2024): 88-97.

[24] Inuwa, Muhammad Muhammad, and Resul Das. "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks." *Internet of Things* 26 (2024): 101162.

[25] Ansar, Nadia, et al. "A Cutting-Edge Deep Learning Method For Enhancing IoT Security." *arXiv preprint arXiv:2406.12400* (2024).

[26] Venkatesan, K., and Syarifah Bahiyah Rahayu. "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques." *Scientific Reports* 14.1 (2024): 1149.

[27] Venkatesan, K., and Syarifah Bahiyah Rahayu. "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques." *Scientific Reports* 14.1 (2024): 1149.

[28] Khan, Maryam Mahsal, and Mohammed Alkhathami. "Anomaly detection in IoT-based healthcare: machine learning for enhanced security." *Scientific Reports* 14.1 (2024): 5872.