International Research Journal of Multidisciplinary Scope (IRJMS), 2025; 6(1):1393-1408 IRJMS

Original Article | ISSN (O): 2582-631X **DOI: 10.47857/irjms.2025.v06i01.02795**

Learning-Based Framework with Optimizations for Enhancing Cyber Security in IoT Use Case

BNV Madhu Babu[1]*, N Pushpalatha[2], Subramanyam M Vadlamani[3], Moligi Sangeetha[4]

[1]CSE Department, Teegala Krishna Reddy Engineering College, Hyderabad, India, [2] CSE Department, Marri Laxman Reddy Institute of Technology and Management, Dundigal, Hyderabad, India, [3]Department of CSE, Anurag Engineering College, SuryapetKodada, Telangana, India, [4]CSE Department, CVR College Of Engineering, Hyderabad, Telangana, India. *Corresponding Author's Email: madhubabucse@tkrec.ac.in

Abstract

Internet of Things (IoT) technology and its applications have new cyberattacks requiring powerful and effective cybersecurity solutions. Although machine learning (ML) techniques are promising to defend cyberspace, most of them depend on predefined hyperparameters, which restrict their effectiveness in defending against a dynamic and evolving threat landscape. To tackle this, we introduce a learning-based framework, subsequently, the integration of an improved hyperparameter optimization technique enhances cybersecurity in IoT domains. Specifically, it exploits an Enhanced Bayesian Optimization (EBO) approach for the optimization of ML models used in attack detection. This technique captures adequate features like tuning covariance hyperparameter dynamically, acquisition functions, parallelization, and cost modeling. In this paper, we propose an algorithm called Learning-based Method with Hyperparameter Optimization for Cyber Attack Detection (LbMHO-CAD), which combines EBO and different ML models, such as Decision Tree, K-Nearest neighbors, Logistic Regression, Support Vector Machine, and Random Forest. These models were evaluated for their generalization ability in detecting a range of cyberattacks, using the UNSW-NB15 benchmark dataset as training data. The experimental results show that the proposed framework 111 14 achieves a maximum accuracy of 97.91% by outperforming the state-of-the-art methods and is 112 able to overcome the issues regarding the data noise and heterogeneity of IoT systems. The proposed research bears a significant generalizability score needed to enhance IoT security under the merged hyperparameter tuning approach and opens avenues for future work on model deep learning integration along with rigorous testing on all-inclusive datatypes.

Keywords: Cyber Security, Enhanced Bayesian Optimization, Hyperparameter Tuning, Internet of Things, Machine Learning.

Introduction

Enabled by the Internet of Things (IoT), a range of applications can be achieved through communication and access between physical and digital objects. For example, smart homes, smart cities, smart transit, and intelligent healthcare systems. This unprecedented application and heterogeneity in protocols, devices, and applications have been leading to vulnerabilities to cyber-attacks. In addition, global standards are insufficient for IoT applications, which is why IoT devices are vulnerable to security threats. At the same time, artificial intelligence (AI) has sprouted as technology with the potential to solve the troubles of the real world. Different approaches, ranging from deep learning (DL) to machine learning (ML), were greatly used in many fields. AI-powered approaches have been ubiquitously adopted to solve challenges in cybersecurity and have proven their utility in making cyberspace more secure. This has led to substantial research on the use of AI for the purpose of cybersecurity. ML techniques have been used to analyze the data from IoT sensors for abnormal patterns to identify the possibility of cyber-attacks. Deep learnings have employed advanced neural networks to accommodate massive traffic in industrial control systems and learning-based methods have been envisaged for cyber-attack detection. ML models based on semi-supervised learning have also been deployed to detect distributed attacks in cyberspace, and they exhibit a good performance when the number of training sample is insufficient. The dynamic assessment of risks in IoT applications has been explored with the implementation of AI-based methods, which may improve security measures.

(Received 10th October 2024; Accepted 28th January 2025; Published 31st January 2025)

Various ML approaches are investigated in literature to secure cyberspace. But it turns out that ML models depend on training data and need hyperparameter tuning to attain better performance. With its ability to analyze massive amounts of data and improve security measures, the potential for machine learning in the IoT has received a lot of interest. Different Machine Learning Methods for IoT Data Analysis provide an overview of insights for processing IoT data in an efficient way (1). Many research studies also investigated cybersecurity algorithms based on machine learning and deep learning, especially for intrusion detection systems and anomaly detection mechanisms in IoT (2-4). Semi-supervised and ensemble learning-based frameworks have been highlighted as necessary to manage evolving cyber threats in industrial control systems and IoT networks (5–7). Deep learning has been rigorously reviewed for its role in IoT security in the context of network anomaly and cyberattack detection (8–10). Intrusion detection approaches have been proposed, which use federated learning and centralized models to enhance the security of IoT-based applications (11). Deep learning has also successfully detected malevolent botnets in IoT networks using diverse approaches (12). Moreover, studies have investigated the applications of cybersecurity frameworks based on machine learning and blockchain technology to improve privacy and security for IoT systems (13-15).

The article emphasizes machine learning techniques for predictive maintenance in manufacturing and industrial IoT and shows that real-time data analytics can lead to proactive maintenance (16). The significance of big data analytics and IoT cybersecurity has also been examined as part of data-driven approaches (17). Also, novel deep learning based methods have been researched to detect DDoS attack in IoT networks, suggesting the potency of artificial intelligence techniques towards addressing the problem of cyber-attacks (18-20). A lot of work has been done to analyze datasets that can be used for detecting intrusions in the network, and one of the most popular is the UNSW-NB15 dataset, which is now being used broadly to compare many cybersecurity models (21-23). Integrating machine learning with blockchain has been studied as a basis for privacy-preserving security frameworks, especially in smart cities and Internet of Things (IoT) applications (24). Choice of feature extraction and machine learning techniques have also been analyzed to showcase potential improvements in intrusion detection in both network and host-based anomaly detection (25-27). Also, there is a growing interest in using these approaches in cybersecurity and IoT security to improve machine learning models (28-30). Gaussian processes have been utilized to optimize deep learning architectures, with promising results in enhancing classification accuracy and model efficiency (31). Several studies also discussed and evaluated attention-based neural networks in terms of their potential application for detecting and classifying cybersecurity threats in IoT environments (32-34).

In conclusion, machine learning and deep learning techniques for IoT security are rapidly becoming mainstream in response to the growing need for cyber risk analytics, as cyber-attacks threaten the robustness of smart infrastructure (35-37). Hybrid security frameworks combining deep learning with blockchain and federated learning methods have been proposed as prospective future research directions (38-40). Another recent related work investigates the use of deep learning approaches for network anomaly detection and intrusion prevention for IoT security (41). The proposed Automatic DDoS detection frameworks utilizing hybrid deep learning models have enhanced performance in detecting and mitigating cyber threats (42). Bayesian optimization-based hyperparameter tuning novel techniques have been suggested for the enhancement of the efficiency of deep learning models in the field of cyber security (43). Convolutional neural networks and attention mechanisms are integrated for the analysis of cyber threats and achieve 48.09% accuracy (44). Moreover, deep learning methods have been explored to secure IoT systems in smart agriculture, suggesting its applicability to secure innovative farming systems against cyber vulnerabilities (45).

In Table 1, we summarize the existing literature on IoT cybersecurity frameworks to examine the utilized methodologies, significant findings, and research gaps.

These studies provide evidence of notable progress, they also highlight the importance of developing strong hyperparameter optimization methods and universal frameworks capable of addressing the diverse problems presented in IoT settings, including data heterogeneity, noise, and scalability.

Table 1: Summary of Literature Review

Reference	Method	Key Findings	Research Gaps
(1)	ML models for IoT network traffic analysis	ML models can monitor network flows and detect inconsistencies effectively.	Focused on detecting vulnerabilities; lacks robust hyperparameter optimization.
(2)	Anomaly detection using IoT sensor data with ML techniques	Detected anomalies in IoT sensor data, demonstrating the potential of supervised learning for attack detection.	Did not explore unsupervised or semi-supervised learning; lacks evaluation on noisy and heterogeneous data.
(3)	Deep learning for industrial control systems	Used advanced DL techniques for detecting cyber-attacks in industrial IoT environments.	Lacks scalability to other IoT use cases; does not address hyperparameter tuning challenges.
(4)	Semi-supervised ML for distributed attack detection	Semi-supervised approaches showed promise for limited training samples in distributed IoT systems.	Limited evaluation on real-world datasets; lacks advanced optimization techniques for improving performance.
(17)	Introduced Edge-IIoTset dataset for IoT security	Dataset covers realistic IoT/IIoT security issues and supports centralized and federated learning.	Frameworks utilizing the dataset fail to address the heterogeneity of data or incorporate efficient parameter tuning.
(31)	UNSW-NB15 dataset for network intrusion detection	A benchmark dataset widely used for training and testing ML models in cybersecurity applications.	Did not incorporate advanced parameter optimization for ML models or compare models under consistent conditions.
(19)	Privacy-preserving ML-based framework for IoT security	Integrated blockchain for ensuring privacy and security in IoT-driven smart cities.	Limited application to specific use cases; lacks generalization to broader IoT environments.
(40)	Machine learning for early DDoS detection in IoT	Demonstrated high performance with ML classifiers for detecting DDoS attacks.	Did not optimize classifiers for IoT traffic or address real-time performance challenges.

Intrusion detection systems have been developed to address challenges in IoT applications, and these systems have been explored using ML techniques (20, 21, 27). In such applications, the dynamic assessment of cyber risks has also been considered essential. AI-based methods have been utilized to assess IoT application risks dynamically, enabling steps to strengthen security primitives (23). The possibility of building intelligent systems using AI and related techniques has been examined (24, 28). A smart system has been proposed for the security of IoT networks integrated with 5G technology (28). Additional contributions include the use of DL-based approaches for IoT monitoring (25), predictive maintenance systems (26), and botnet discovery in IoT networks using DL methods (30).

Various ML techniques have been identified as effective tools for securing cyberspace. However, it has been observed that the performance of ML models depends significantly on the availability of high-quality training data, and hyperparameter tuning plays a crucial role in achieving optimal results. In this study, hyperparameter estimation has been incorporated to leverage cutting-edge techniques and improve performance.

The following are our contributions to this publication. We suggested a structure for the automatic detection of cyberattacks along with an enhanced Bayesian Optimization (BO) technique for parameter optimization. We presented a learning-based method with hyperparameter Optimization for Cyber Attack Detection (LbMHO-CAD) that automatically detects cyber-attacks. We developed an application to implement the framework and underlying algorithm. Experimental evaluation has shown that the suggested framework performs better than the current techniques. The remainder of the work is structured as follows: Part 2 examines the literature on modern machine learning (ML) and alternative strategies for preventing cyberattacks in Internet of Things applications. Section 3 presents our framework and its underlying mechanics. Section 4 shows the outcomes of our experiment. While Section 6 offers conclusions and outlines potential areas for future improvements, Section 5 discusses the shortcomings of the suggested framework.

Methodology

The automated detection framework suggested for cyber-attacks includes an enhanced optimization method for hyperparameter optimization that leverages accuracy in attack detection. Subsequent sections provide more details.

Problem Definition

The main problem is detecting different kinds of attacks or intrusions occurring in real-time with improved accuracy. Moreover, the problem of hyperparameter tuning based on the given dataset is also considered.

The Framework

A proposed framework, shown in Figure 1, exploits ML models to detect cyber-attacks in IoT use cases automatically. Unlike existing intrusion detection methods such as (32-34), we focused on improving the Bayesian optimization (BO) method for parameter tuning. Figure 2 shows an overview of the enhanced BO method used in the proposed framework. Hyperparameter tuning plays a crucial role in improving the performance of ML models (44, 45). The rationale is that hyperparameter optimization is done based on the given dataset. Since each dataset is different in real-world applications, optimization of hyperparameters of ML models assumes significance.

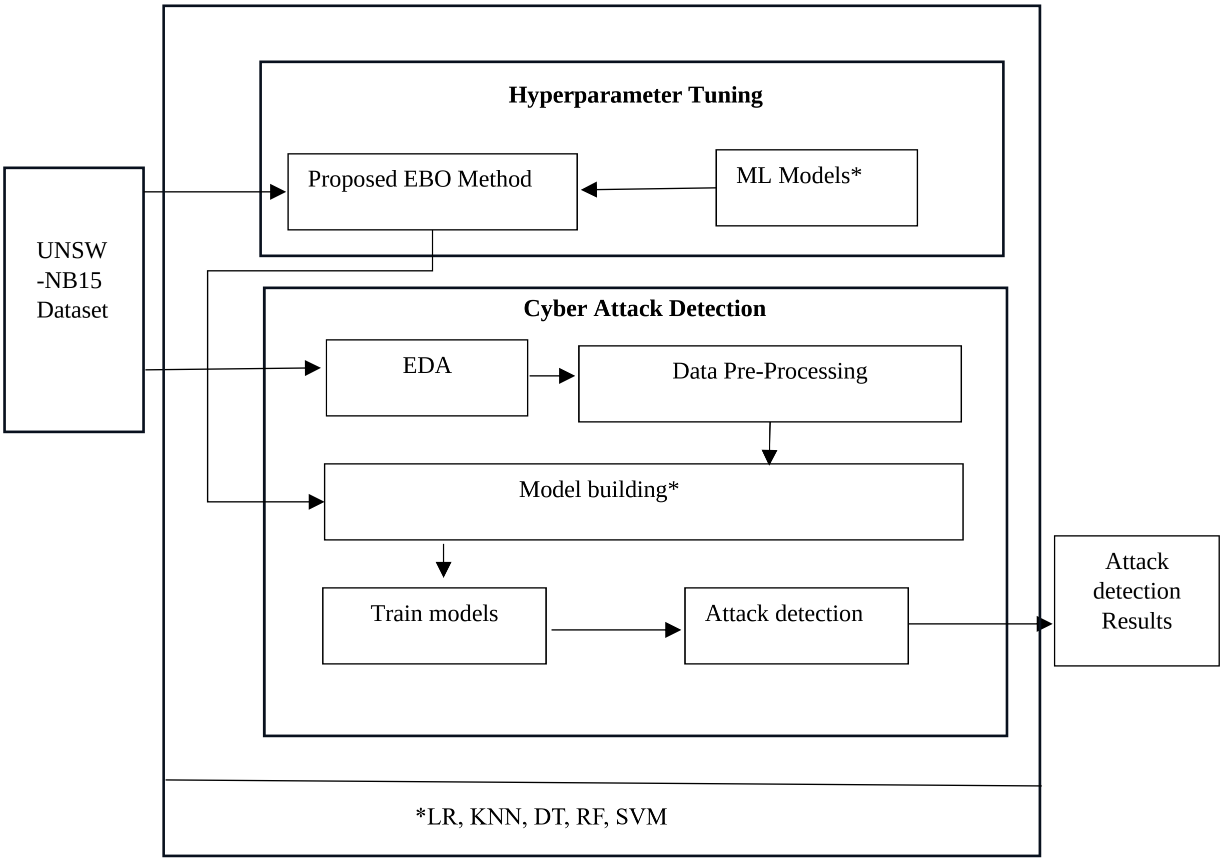

Figure 1: Proposed Framework for Automatic Detection of Cyber Attacks

The framework takes the UNSW-NB15 dataset as input. This dataset has ground truth and test instances, as discussed in Section 3.6. The machine learning models employed in this study include

Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), k-Nearest Neighbor (KNN), and Logistic Regression (LR). These models are subjected to hyperparameter tuning using the proposed enhanced BO method. The EBO method takes the UNSW-NB15 dataset as input and tunes the parameters of ML models.

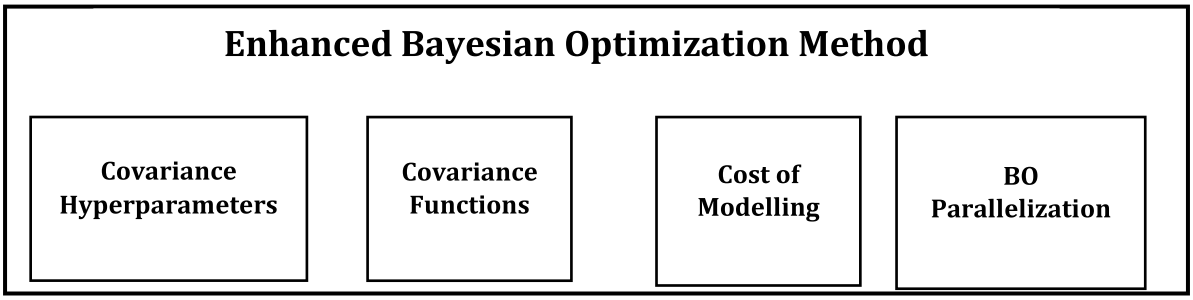
Enhanced Bayesian Optimization Method
Covariance Hyperparameters
Covariance Functions
Cost of Modelling
BO Parallelization

Figure 2: Overview of Enhanced BO Method for Hyperparameter Optimization

The EBO method has different considerations like covariance hyperparameters, covariance functions, cost of modeling, and BO parallelization. Section 3.4 provides more details on the EBO method and its modus operandi. After parameter tuning, the proposed framework performs Exploratory Data Analysis (EDA) on the UNSW-NB15 dataset to know data dynamics. EDA helps the framework perform suitable data pre-processing operations like duplicate checking, missing values, and encoding. After pre-processing, the models subjected to EBO are used in the training phase to gain knowledge, and then they are used to detect cyber-attacks.

The Enhanced Bayesian Optimization (EBO) method builds on classic Bayesian Optimization (BO) methods by adding parallelization, improved tuning of the covariance function, and improved cost modeling. Unlike traditional BO using fixed covariance functions and sequential evaluations, EBO intelligently adjusts to dataset properties with the help of Monte Carlo simulations, all-in-one for acquisition function estimation, this ensures strong hyperparameter tuning irrespective of dataset dimensions. Additionally, EBO employs parallel batch evaluations, which greatly improves the computational time at no compromise on optimization accuracy. Taken together, EBO outperforms other optimization methods such as grid search, random search, and Tree-structured Parzen Estimators (TPE) because of its explicit modeling of the spatial posterior distribution over objective functions, enabling it to manage noise well and capture complex data dynamics. EBO is thus especially well-suited for IoT deployment, where raw data may be noisy and heterogeneous.

Machine Learning Models

Different models used in this research for automatic detection of cyber-attacks are provided in Table 2. These are supervised learning techniques.

Table 2: Shows Models Used in the Empirical Study

ML Model	Description
Decision Tree (DT)	It is a tree-based model that is meant for attack classification
K-Nearest Neighbour (KNN)	This model leverages the nearest neighbour approach to detect intrusions
Logistic Regression (LR)	Based on probability theory, this model can detect intrusions.
Support Vector Machine (SVM)	This model exploits hyperplane to distinguish attack traffic from normal traffic.
Random Forest (RF)	This model makes use of several trees with an ensemble phenomenon.

Enhanced Bayesian Optimization

Finding the function f(x) for a limited set χ that we take on a subset of R^D is crucial in BO. In contrast to previous optimizations, BO creates a probabilistic model for f(x) and uses the model to inform decisions. It is not limited to using estimations of the local gradient and Hessian; rather, it considers all prior assessments of f(x). Thus, to minimize computing costs, it can identify non-convex functions. Because f(x) assessments need machine learning training, they are growing more costly. However, this expense is acceptable because the model produces accurate conclusions. When using BO, two crucial decisions must be made: selecting a prior function that accounts for any presumptions and developing a utility function to determine the subsequent assessment point. Given its strength, we considered representing the prior distribution of functions, the Gaussian process (GP). It has a structure like $f: \chi \longrightarrow R$. Table 3 shows the notations used in the paper.

Table 3: Notations Used in Hyper-parameter Optimization Using Enhanced BO

Notation	Meaning
χ	Denotes bounded set
$y = [y_1, y_2, \dots, y_N]^T$	Covariance matrix
v	Denotes observation noise
m	Indicates a constant mean
k	Value used to balance exploitation and exploration
$f(x)$	Function
$a(X)$	Value acquired from different observations
$\Phi(\cdot)$	Indicates cumulative distribution function
GP	Prior distribution
$\theta_{1:D}$	Scales of D length
θ_0	Indicates covariance amplitude
$y_n \sim N(f(X_n), v)$ and v	Function observation with variance of noise
$(X): \chi \to R^+$	Indicates a duration function
R^D	Indicates a subset

$\{X_n \in \chi\}_{n=1}^N$ GP has the property of creating multivariate Gaussian distribution on R^N. The value of the function $f(X_n)$ is the nth point from a finite set of points (N). This distribution's elegant marginalization properties facilitate the calculation of conditions and marginals. For functions, a mean function m:χ→R and a covariance function $K: \chi \times \chi \to R$ yield the final distribution. For further information on Gaussian processes (42).

Enhanced Bayesian Optimization (EBO) is an extension of Bayesian Optimization (BO) for hyperparameter tuning in data science that makes some necessary improvements. Improvements such as dynamic tuning of covariance hyperparameters for more accurate modeling of complex inter-data dependencies, advanced acquisition strategies like a monte-carlo-optimized expected improvement (EI) and parallelized multiple batch evals allow for substantially lower computation time. Moreover, EBO also utilizes cost modeling to dynamically strike a balance between exploration and exploitation, thus maintaining both computational efficiency and accuracy of the search results. This pendulum motion of refined optimization makes a continual evolution in the machine learning techniques used in this experiment, namely Decision Tree, K-Nearest Neighbors, Logistic Regression, Support Vector Machine, and Random Forest, turning them to the best based on the respective dataset of IoT and improving the detection of cyberattacks at its best performance.

BO and Its Acquisition Functions

Our observations take the form $\{X_n, y_n\}_{n=1}^N$, when the introduction of noise takes the form
$y_n \sim N(f(X_n), v$, and f(x) is, as we thought, from the Gaussian process prior. Subsequently, an acquisition function $a: \chi \to R^+$ascertains the subsequent point to be assessed using proxy optimization. It is represented as $X_{next} = argmax_X \, a(X)$According to previous findings and GP hyperparameters. The expression for this dependence is $a(X; \{X_n, y_n\}, \theta)$. Regarding the acquisition function, there are several choices. However, such functions are dependent upon the model via the variance function for the Gaussian process prior, represented as $\sigma^2(X; \{X_n, y_n\}, \theta)$, and the predictive mean function, $\mu(X; \{X_n, y_n\}, \theta)$. In this sense, the current best value is calculated using $X_{best} = argmin_{X_n} f(X_n)$, where Φ(•) stands for the cumulative distribution function. Eq. 1 expresses the analytical computation that is done to maximize improvement probability.

$a_{P1}(X;\{X_n,y_n\},\theta)=\emptyset(\gamma(X)),\quad \gamma(X)=\frac{f(X_{best})-\mu(X;\{X_n,y_n\},\theta)}{\sigma(X;\{X_n,y_n\},\theta)}.$ [1]

As an alternative, anticipated improvement (EI) can be calculated using Eq. 2.

$\alpha_{EI}(X;\{X_n,y_n\},\theta)=\sigma(X,\{X_n,y_n\},\theta)\left(\gamma(X)\emptyset(\gamma(X))+N(\gamma(X);0,1)\right)$ [2]

Recently, the higher confidence level for GP has been used to implement the acquisition functions given in Eq. 3.

$\alpha_{LCB}(X;\{X_n,y_n\},\theta)=\mu(X;\{X_n,y_n\},\theta)-k\sigma(X;\{X_n,y_n\},\theta)$ [3]

A configurable parameter called k strikes the right balance between exploration and exploitation. In this paper, EI is taken into account.

Covariance Hyperparameters and Covariance Functions

GP, based on the covariance function, supports a wealth of distributions on functions. In this case, determining relevance is crucial. Equation 4 is used to compute this.

$K_{SE}(X,X\grave{})=\theta_0 exp\{-\frac{1}{2}r^2(X,X\grave{})\}r^2(X,X\grave{})=\sum_{d=1}^{D}\frac{(x_d-\grave{x}_d)^2}{\theta_d^2}$ [4]

The 5/2 kernel is utilized to achieve more improvements, as stated in Equation 5.

$K_{M52}(X,X\grave{})=\theta_0\left(1+\sqrt{5r^2(X,X\grave{})}+\frac{5}{3}r^2(X,X\grave{})\right)ex\,p\left\{-\sqrt{5r^2(X,X\grave{})}\right\}$ [5]

As a result, sample functions that lack the squared exponential's smoothness become progressively differentiable. Upon determining the nature of covariance, hyperparameter management becomes crucial. The hyperparameters for the D + 3 Gaussian process consist of the constant mean m, the observation noise v, and the covariance amplitude θ_0. The most popular method for maximizing Gaussian process-related parameters is stated as

$p(y|\{X_n\}_{n=1}^{N},\theta,v,m)=N(y|m1,\sum_\theta\quad+v1).$

Therefore, Eq. 6 expresses an integrated acquisition function.

$\hat{\alpha}(X;\{X_n,y_n\})=\int\quad a(X;\{X_n,y_n\},\theta)p(\{X_n,y_n\}_{n=1}^{N})d\theta$ [6]

Every observation is necessary for both θ and a(X). Attaining generalization in hyperparameters is crucial for emotional intelligence. A Monte Carlo estimate is used to arrive at this figure. To efficiently obtain samples, slice mapping is employed (35).

Considering Modelling Costs

BO must take modeling costs into account when optimizing quickly. We optimized for EI per second, which yields points without generating a significant amount of overhead. We hypothesize that while the true objective function f(X) and the duration function $(X):\chi\rightarrow R^+$ are independent, they aid in capturing via GP fluctuations for multi-task learning. When the independence requirement is met, calculating the inverse duration expected to compute EI every second is less complicated.

Parallelizing Bayesian Optimization

Now that multi-core computing has become commonplace, BO methods may be parallelized. We decide which point needs to be analyzed next using batch parallelism. Experiments are repeated as using the same function more than once is impossible. Additionally, we suggested a sequential approach to compute Monte Carlo estimations related to the acquisition function, which uses the tractable inference capabilities of GP. Given N evaluations and $\{X_n,y_n\}_{n=1}^{N}$ as generating data, it is plausible that J evaluations, represented as $\{X_j\}_{j=1}^{J}$, are waiting at various places. Considering all possible outcomes related to pending assessments, a new point is selected based on the projected acquisition function.

$\hat{a}(X;\{X_n,y_n\},\theta,\{X_j\})=\int_{R^J}\alpha(\mathrm{X};\{X_n,y_n\},\theta,\{X_j,y_j\})\,p(\{X_j\}_{j=1}^{J},\{X_n,y_n\}_{n=1}^{N})\mathrm{dy1....dyj}$ [7]

The expectation of a(x) given a J-dimensional Gaussian distribution—whose covariance and mean can be easily found—is all at stake in this situation. Computed expected acquisition with samples is more accessible when the covariance hyperparameter is considered. While we have demonstrated the high success rate of the Monte Carlo estimate technique (43).

Algorithm Design

Based on EBO and ML models, we proposed an algorithm that automatically detects cyber-attacks. The algorithm is called Learning based Method with Hyperparameter Optimization for Cyber Attack Detection (LbMHO-CAD).

```
Algorithm: Learning-based Method with Hyperparameter Optimization for Cyber Attack Detection
(LbMHO-CAD)

Inputs
UNSW-NB15 dataset D
ML models M
Output
Attack detection results

•    Begin
Hyperparameter optimization
•    For each model m in M
•    Update m using the EBO method
•      Add m to M'
•    End For
Pre-Processing
•    Status⍰EDA(D)
•    IF Status reflects need for improving data Then
•      Remove duplicates
•      Treat missing values
•      Scaling
•    End If
•    (T1, T2)⍰DataSplit(D)
Attack Detection
•    For each model m' in M'
•      Train m' with T1
•      Use m' to detect cyber attacks
•      Display attack detection results
•    End For
•    End
```

Algorithm 1: Learning based Method with Hyperparameter Optimization for Cyber Attack Detection

As presented in Algorithm 1, the proposed algorithm inputs UNSW-NB15 dataset D and ML model M. It performs hyperparameter tuning using the proposed EBO method. Based on EDA results, the algorithm determines whether the data needs to be improved by removing duplicates, treating missing values, and scaling. Then, the algorithm has the provision to train updated models and perform attack detection.

Dataset Details

The UNSW-NB15 dataset was collected from a previous research for empirical study (31). It contains nine kinds of cyber-attacks that commonly occur in different applications, including IoT use cases. The dataset has 175341 instances for training and 82332 instances for testing. It is one of the widely used datasets for cyber security research (32, 34).

Evaluation Procedure

The suggested method is assessed using several performance metrics from the scenarios depicted in Figure 3.

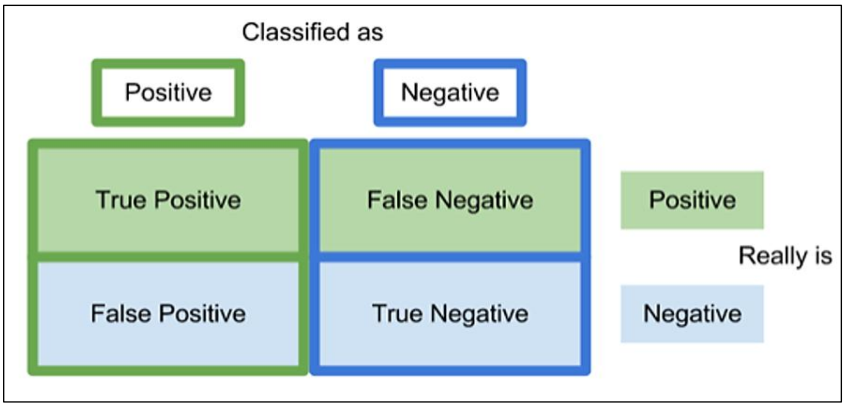

Figure 3: Confusion Matrix

Performance metrics are applied to determine the efficiency of the proposed framework. They are as in Eq. 8, Eq. 9, and Eq. 10.

Precision = $\frac{TP}{TP+FP}$ [8]

Recall = $\frac{TP}{TP+FN}$ [9]

Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$ [10]

These metrics are used in the evaluation of the ML models.

Results and Discussion

This section displays the results of the proposed framework's experiments. The results are divided into three categories: EDA, performance of the proposed algorithm and performance comparison with prior works. The effectiveness of the suggested algorithm with different ML models is compared against prior works (36-40). We observed from the empirical study that our method outperforms existing models due to the enhanced BO that could optimize hyperparameters for the UNSW-NB15 dataset.

Exploratory Data Analysis

The UNSW-NB15 dataset was subjected to EDA to determine its distribution. EDA helped determine the need for duplicate removal, treating missing values, and scaling. This section presents different aspects of the data and its distribution dynamics. As presented in Figure 4, the distribution of attacks and normal instances in the UNSW-NB15 dataset arevisualized. As presented in Figure 5, the distribution of different services in the UNSW-NB15 dataset is visualized. Figure 6 visualizes the distribution of different communication or transaction protocols in the UNSW-NB15 dataset. As presented in Figure 7, the results of bivariate analysis are provided. It reflects the distribution of visualized attack categories and services in the UNSW-NB15 dataset. Figure 8 visualizes the distribution of data in terms of different attack categories in the UNSW-NB15 dataset. As presented in Figure 9, the percentage of normal and attack instances in the UNSW-NB15 dataset is visualized.

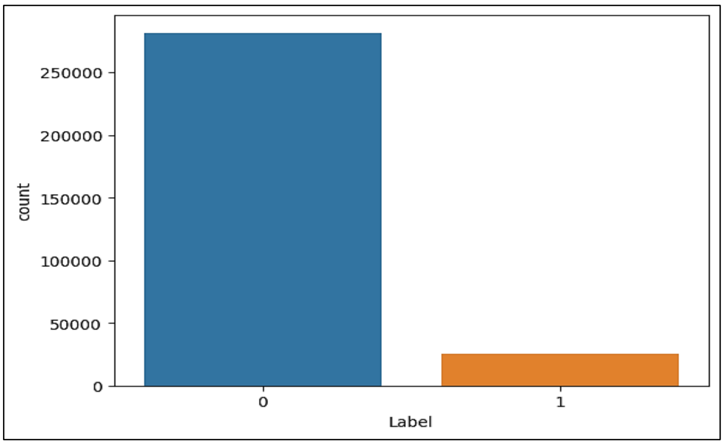

Figure 4: Attack and Normal Traffic Distribution in the Dataset

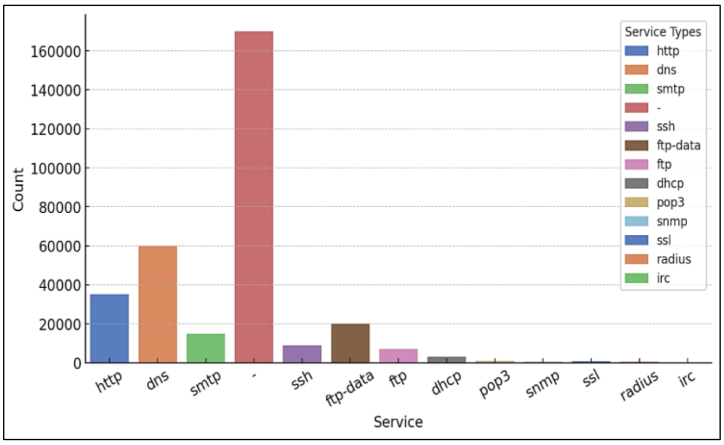

Figure 5: Data Distribution Dynamics of Different Services

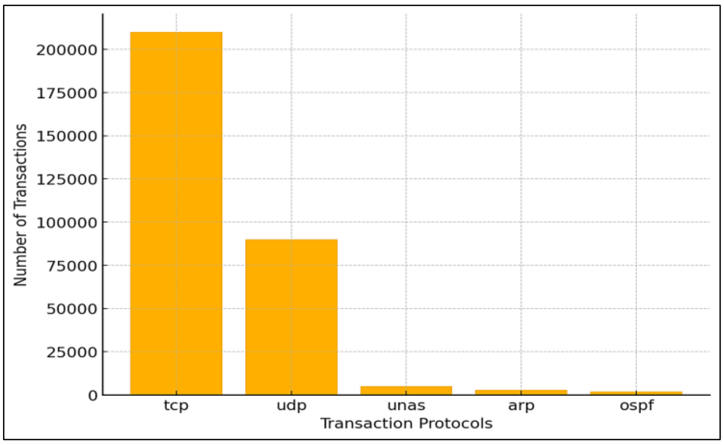

Figure 6: Data Distribution Dynamics about Different Protocols

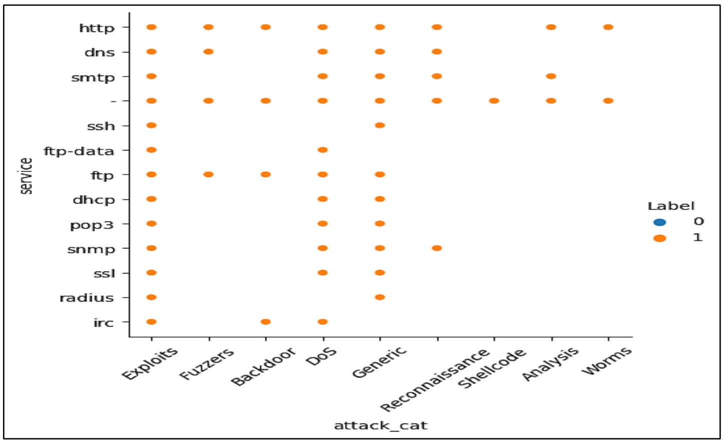

Figure 7: Bivariate Analysis Reflecting Different Attack Categories against Services

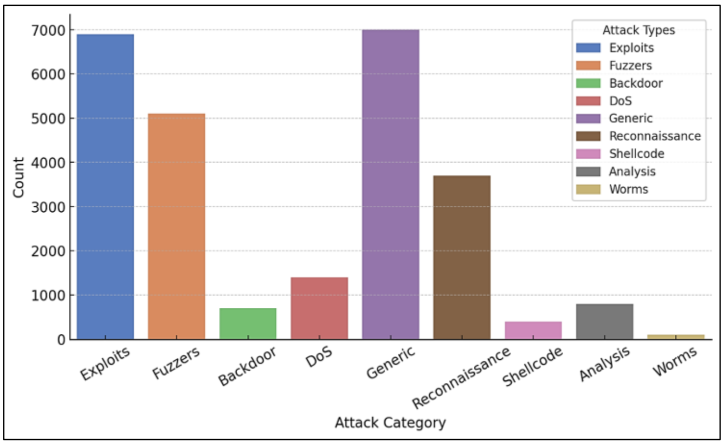

Figure 8: Data Distribution against Various Attack Categories

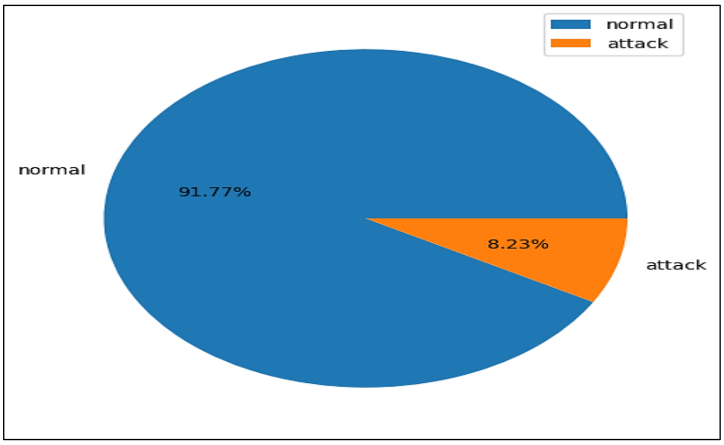

Figure 9: Percentage of Data about Normal and Attack Traffic

Performance of ML Models Optimized by EBO

This section shows every ML model employed in this study. These models are optimized using the EBO method. Due to parameter optimization based on the UNSW-NB15 dataset, the underlying ML models could perform better in terms of efficient cyber-attack detection. Table 4 presents the performance exhibited by various models.

Table 4: Performance of ML Models with EBO Method for Hyperparameter Tuning

Attack Detection Model	**Performance (%)**		
	Precision	**Recall**	**Accuracy**
kNN	0.8864	0.8561	0.9791
RF	0.8499	0.9026	0.9788
DT	0.8337	0.8789	0.9755
SVM	0.7661	0.8485	0.9661
LR	0.7640	0.8190	0.9642

The table shows the performance of different ML models for attack detection along with the EBO method used for hyper-parameter tuning. We compare precision, recall, accuracy across KNN, RF, DT, SVM, and LR metrics. RF has the highest recall, and KNN has the highest precision. Across models, accuracy is reliably high.

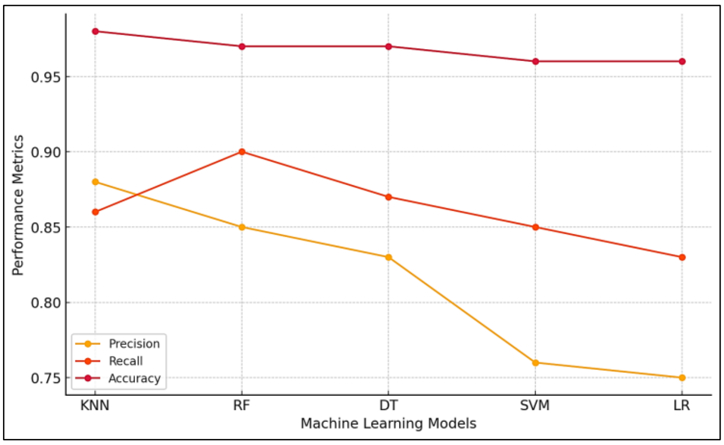

Figure 10: Attack Detection Performance Comparison of ML Models Optimized by EBO

As presented in Figure 10, the performance of ML models optimized by EBO for hyperparameter tuning is provided. Each model showed different performance due to their underlying detection methodology. The least precision is exhibited by LR with 76.40%. The highest precision is achieved by the KNN model with 88.64%. Similarly, the least recall is shown by LR with 81.90%, and the highest recall observed in 90.26%, exhibited by RF. Regarding accuracy, the least performance is demonstrated by LR with 96.42% and the highest accuracy is exhibited by KNN with 97.91%.

Performance Comparison with State of the Art

This section presents experimental results. The existing approach is taken from prior works. The proposed EBO-based approach is compared against the existing approach. Table 5 shows proposed approach compared with existing approach.

Table 5: Model Performance Comparison

Attack Detection Model	Accuracy (%) Existing Approach	Proposed EBO Approach
KNN	94.57 (36)	97.91
RF	91.66 (37)	97.88
DT	85.83 (38)	97.55
SVM	93.3 (39)	96.61
LR	95.34 (40)	96.42

Table compares the accuracy of other machine learning algorithms for attack detection based on existing and proposed EBO approach. The EBO approach enhances all models by a large margin. KNN delivers the topmost accuracy (97.91%) and is trailed in accuracy by RF and DT. This new proposed approach significantly improves the accuracy over the existing metrics.

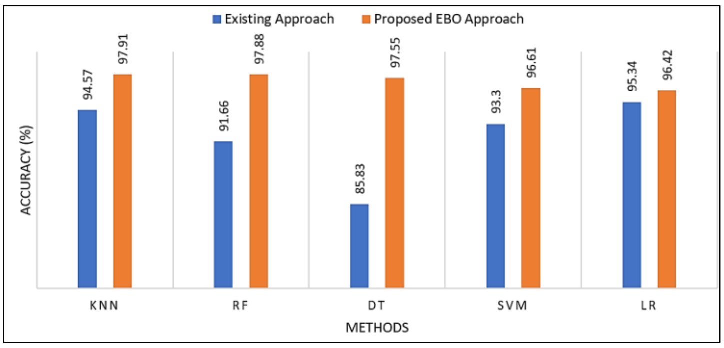

Figure 11: Performance Comparison between Proposed EBO-Based ML Models and Existing ML Models

Figure 11 shows the results of ML models optimized using EBO for hyperparameter tuning compared against existing ML models. Each model showed different performance due to their underlying detection methodology. Accuracy is the measure used for comparison. Higher accuracy indicates better attack detection performance. The existing approach with KNN showed 94.57% accuracy, while the proposed approach with KNN exhibited 97.91% accuracy. RF with the existing approach showed 91.66% while the proposed method showed 97.8% accuracy. DT of the existing approach achieved 85.83% while its proposed counterpart exhibited 97.55% accuracy. The existing approach with SVM showed 93.30% while the proposed method with SVM showed 9.61% accuracy. LR exhibited 95.34% with the existing method, while the proposed method with LR showed 9.42% accuracy. Based on the findings, it is noted that the suggested ML framework with EBO for hyperparameter optimization could outperform existing methods. Table 6 provide quality analysis.

Table 6: Qualitative Analysis

Method	Dataset Used	Technique	Advantages	Disadvantages
(4)	IoT-generated data	Semi-supervised ML	Effective for small, imbalanced datasets	Limited scalability to diverse datasets
(3)	Industrial IoT data	Deep learning-based anomaly detection	High accuracy for large-scale data	High computational cost; limited hyperparameter tuning
(17)	Edge-IIoTset	Centralized/federated ML	Realistic dataset for IoT security	Lacks hyperparameter optimization and real-time application support
Proposed Framework	UNSW-NB15	EBO with ML (DT, KNN, RF, SVM, LR)	High accuracy (97.91%), robust hyperparameter tuning, adaptable to noisy IoT data	Evaluation limited to UNSW-NB15; not yet validated on additional datasets

To summarize the importance of comparison, this table presented to discuss all the desired aspects between the proposed framework and state-of-the-art techniques for IoT cyberattack detection. This summarizes the datasets used, techniques adopted, benefits, and drawbacks of each method. The developed framework that utilizes Enhanced Bayesian Optimization (EBO) using machine learning models is giving improved accuracy (97.91%) along with hyperparameter tuning, which is effective in noisy IoT data. On the other hand, deep learning or semi-supervised approaches cannot efficiently perform hyperparmeter optimization or demand a high amount of computational resources (4, 14, 45). The evaluation of the proposed framework has been only on the UNSW-NB15 dataset with further evaluation on other datasets needed. This research presents an ML architecture to refer, enhanced detection of cyber-attacks for more robust cybersecurity solutions in the IoT use cases. The framework comprises a combination of machine-learning models, targeting the detection of attack patterns, along with hyperparameter tuning for each model. Using Enhanced Bayesian Optimization (EBO) allows the framework to show significant improvement over traditional hyperparameter tuning methods. It dynamically varies key elements like covariance hyperparameters and acquisition functions to tailor the models according to the specialized nature of IoT datasets. Moreover, the obtained tuning also proves that it can adjust noisy and heterogeneous data from IoT environments, which makes it accuracy and reliability. As an example, the accuracy of the K-Nearest Neighbors (KNN) model was 97.91%, which indicates significant influence of EBO in improving performance. In addition, using Exploratory Data Analysis (EDA) guarantees that steps for data preprocessing, like duplicate deletion, handling of missing values, and scaling, are correctly configured to the dataset. This framework is strong and powerful to detect different varieties of cyber-attack using EBO and different machine learning models used was Decision Tree, K-Nearest Neighbors, Logistic Regression, Support Vector Machine, Random Forest. This, paired with the EBO's exploration and exploitation balance for parameter optimization, establishes the framework as a scalable mitigation solution for IoT applications against the evolving threat landscape.

Conclusion

We suggested a structure for the automatic detection of cyberattacks. We enhanced the Bayesian Optimization (BO) technique for parameter optimization. Our Enhanced Bayesian Optimization (EBO) method has different considerations like covariance hyperparameters, covariance functions, cost of modeling, and BO parallelization. Based on EBO and ML models, we proposed an algorithm that automatically detects cyber-attacks. The algorithm is called Learning based Method with Hyperparameter Optimization for Cyber Attack Detection (LbMHO-CAD). It performs hyperparameter tuning using the proposed EBO method. Based on EDA results, the algorithm determines whether the data needs to be improved by removing duplicates, treating missing values and scaling. Then the algorithm has provision to train updated models and perform attack detection. We used a benchmark dataset known as UNSW-NB15 for our empirical study. Our experimental results have revealed that our EBO-based approach outperformed existing ML techniques. Our method achieved the highest accuracy at 97.91%. In the future, we work on deep learning models along with the proposed EBO method to improve our framework for efficient cyberattack detection. UNSW-NB15 is a comprehensive dataset to validate IoT cybersecurity frameworks, and it is important to verify the generalizability of the proposed framework in various IoT environments. We will evaluate our framework on diversified datasets, including CICIDS2017, ToN_IoT, and Bot-IoT in the future work. Such evaluations will however illustrate the strength of the proposed Enhanced Bayesian Optimization (EBO) method and adaptability over different IoT use cases.

Limitations

Although the proposed framework presents notable accuracy and efficiency enhancements, certain limitations exist. The first limitation is that the experiments were conducted based on the UNSW-NB15 dataset, which may cause possible bias due to the fact that the dataset is not a complete representative for the diverse attack patterns and versatile network environments present in real-world IoT scenarios. As such, assessing the framework on other datasets is necessary to confirm generalizability. Second, the machine learning models used, for example Logistic Regression and Decision Tree, are unlikely to detect complex non-linear relationships that may exist within some types of attacks. More advanced models, such as deep learning, may improve performance but require more computational power. Finally, although EBO makes hyperparameter selection more performant, it still has more complexity than other methods (like grid or random search), which may complicate its adoption for real-time applications in resource-poor connected devices. The limitations in current data diversity and models as well as the EBO process will be the focus of future research studies to improve upon all of these considerations.

Abbreviations

IoT: Internet of Things, AI: Artificial Intelligence, ML: Machine Learning, BO: Bayesian Optimization, EBO: Enhanced Bayesian Optimization, EDA: Exploratory Data Analysis, GP: Gaussian process.

Acknowledgement

Nil.

Author Contributions

All authors contributed to the study's conception and design. Material preparation, data collection, and analysis were performed by Dr. Bnv Madhu Babu, Dr N Pushpalatha, Subramanyam M Vadlamani and Moligi Sangeetha. The first draft of the manuscript was written by S Subramanyam M Vadlamani. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Conflict of Interest

The authors declare no conflicts of interest.

Ethics Approval

This research does not involve humans or animals, so no ethical approval is required.

Funding

The authors received no financial support for this research.

References

1. Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. Machine learning for Internet of Things data analysis: A survey. Digital Communications and Networks. 2018 Aug 1;4(3):161-75. doi: 10.1016/j.dcan.2017.10.002
2. Hasan M, Islam MM, Zarif MI, Hashem MM. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things. 2019 Sep 1;7:100059. . doi: 10.1016/j.iot.2019.100059
3. Al-Abassi A, Karimipour H, Dehghantanha A, Parizi RM. An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access. 2020 May 4;8: 83965-83973. doi: 10.1109/ACCESS.2020.2992249
4. Rathore S and Park JH. Semi-supervised learning based distributed attack detection framework for IoT. Applied Soft Computing. 2018 Nov 1;72:79-89. doi: 10.1016/j.asoc.2018.05.049
5. Cui L, Yang S, Chen F, Ming Z, Lu N, Qin J. A survey on application of machine learning for Internet of Things. International Journal of Machine Learning and Cybernetics. 2018 Aug;9:1399-417. doi: 10.1007/s13042-018-0834-5
6. Geetha R, Thilagam T. A review on the effectiveness of machine learning and deep learning algorithms for cyber security. Archives of Computational Methods in Engineering. 2021 Jun;28(4):2861-79.
7. Da Costa KA, Papa JP, Lisboa CO, Munoz R, de Albuquerque VH. Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks. 2019 Mar 14;151:147-57.
8. Liang F, Hatcher WG, Liao W, Gao W, Yu W. Machine learning for security and the internet of things: the good, the bad, and the ugly. Ieee Access. 2019 Oct 22;7:158126-47.
9. Adi E, Anwar A, Baig Z, Zeadally S. Machine learning and data analytics for the IoT. Neural computing and applications. 2020 Oct;32:16205-33.
10. Sarker IH, Kayes AS, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big data. 2020 Dec;7:1-29.
11. Ullah Z, Al-Turjman F, Mostarda L, Gagliardi R. Applications of Artificial Intelligence and Machine Learning in Smart Cities. Computer Communications. 2020; 154:313–323.
12. Koroniotis N, Moustafa N, Sitnikova E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems. 2020 Sep 1;110:91-106.
13. Bagaa M, Taleb T, Bernabe JB, Skarmeta A. A machine learning security framework for iot systems. IEEE Access. 2020 May 21;8:114066-77.
14. Shafiq M, Tian Z, Bashir AK, Du X, Guizani M. CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet of Things Journal. 2020 Jun 15;8(5):3242-54.
15. Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MS. Application of big data and machine learning in smart grid, and associated security concerns: A review. Ieee Access. 2019 Jan 24;7:13960-88.
16. Makkar A, Garg S, Kumar N, Hossain MS, Ghoneim A, Alrashoud M. An efficient spam detection technique for IoT devices using machine learning. IEEE Transactions on Industrial Informatics. 2020 Jan 23;17(2):903-12.
17. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022 Apr 8;10:40281-306.
18. Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things. 2020 Sep 1;11:100227.
19. Kumar P, Kumar R, Srivastava G, Gupta GP, Tripathi R, Gadekallu TR, Xiong NN. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering. 2021 Jun 16;8(3):2326-41.
20. Rahman MA, Asyhari AT, Leong LS, Satrya GB, Tao MH, Zolkipli MF. Scalable machine learning-based intrusion detection system for IoT-enabled smart

cities. Sustainable Cities and Society. 2020 Oct 1;61:102324.

21. Wang M, Zheng K, Yang Y, Wang X. An explainable machine learning framework for intrusion detection systems. IEEE Access. 2020 Apr 16;8:73127-41.
22. Chhabra GS, Singh VP, Singh M. Cyber forensics framework for big data analytics in IoT environment using machine learning. Multimedia Tools and Applications. 2020 Jun;79:15881-900.
23. Radanliev P, De Roure D, Walton R, Van Kleek M, Montalvo RM, Maddox LT, Santos O, Burnap P, Anthi E. Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Applied Sciences. 2020 Nov;2:1-8.
24. Roldán J, Boubeta-Puig J, Martínez JL, Ortiz G. Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. Expert Systems with Applications. 2020 Jul 1;149:113251.
25. Tran MQ, Elsisi M, Liu MK, Vu VQ, Mahmoud K, Darwish MM, Abdelaziz AY, Lehtonen M. Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. IEEE Access. 2022 Feb 22;10:23186-97.
26. Ayvaz S, Alpay K. Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. Expert Systems with Applications. 2021 Jul 1;173:114598.
27. Gad AR, Nashat AA, Barkat TM. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access. 2021 Oct 15;9:142206-17.
28. Rathore S, Park JH, Chang H. Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT. IEEE access. 2021 May 3;9:90075-83.
29. Al-Garadi MA, Mohamed A, Al-Ali AK, Du X, Ali I, Guizani M. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE communications surveys & tutorials. 2020 Apr 20;22(3):1646-85.
30. Khan S, Mailewa AB. Discover Botnets in IoT Sensor Networks: A Lightweight Deep Learning Framework with Hybrid Self-Organizing Maps. Microprocessors and Microsystems. 2023; 97:1–12.
31. UNSW_NB15 Dataset. https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15
32. Moustafa N and Slay J. UNSW-NB15: A Comprehensive Dataset for Network Intrusion Detection Systems. Military Communications and Information Systems Conference (MilCIS). IEEE. 2015:1-6. http://dx.doi.org/10.1109/MilCIS.2015.7348942
33. Moustafa N and Slay J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective. 2016 Apr 4;25(1-3):18-31.
34. Moustafa N, Slay J, Creech G. Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. IEEE Transactions on Big Data. 2017 Jun 14;5(4):481-94.
35. Cil AE, Yildiz K, Buldu A. Detection of DDoS attacks with feed forward based deep neural network model. Expert Systems with Applications. 2021 May 1;169:114520.
36. Aamir M, Zaidi SM. Clustering based semi-supervised machine learning for DDoS attack classification. Journal of King Saud University-Computer and Information Sciences. 2021 May 1;33(4):436-46.
37. Ahuja N, Singal G, Mukhopadhyay D, Kumar N. Automated DDoS Attack Detection in Software-Defined Networking. Journal of Network and Computer Applications. 2021; 187:1–12.
38. Tuan TA, Long HV, Son LH, Kumar R, Priyadarshini I, Son NT. Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence. 2020 Jun;13(2):283-94.
39. Gaur V, Kumar R. Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering. 2022 Feb;47(2):1353-74.
40. Brochu E, Cora VM, De Freitas N. A tutorial on Bayesian optimization of expensive cost functions, with application to active user modeling and hierarchical reinforcement learning. arXiv preprint arXiv:1012.2599. 2010 Dec 12. https://arxiv.org/abs/1012.2599
41. Rasmussen CE and Williams CKI. Gaussian Processes for Machine Learning. MIT Press. 2006;2(3):4.
42. Ginsbourger D, Le Riche R. Dealing with Asynchronicity in Parallel Gaussian Process-Based Global Optimization. HAL Archives. 2010. https://hal.science/hal-00507632/
43. Sameen MI, Pradhan B, Lee S. Application of convolutional neural networks featuring Bayesian optimization for landslide susceptibility assessment. Catena. 2020 Mar 1;186:104249.
44. Ranjit MP, Ganapathy G, Sridhar K, Arumugham V. Efficient Deep Learning Hyperparameter Tuning Using Cloud Infrastructure: Intelligent Distributed Hyperparameter Tuning with Bayesian Optimization in the Cloud. IEEE International Conference on Cloud Computing (CLOUD). 2019; 12: 520–522.
45. Wang Y, Wang H, Peng Z. Rice diseases detection and classification using attention based neural network and bayesian optimization. Expert Systems with Applications. 2021 Sep 15;178:114770.