IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 April 2024, accepted 7 June 2024, date of publication 12 June 2024, date of current version 30 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3413600

RESEARCH ARTICLE

Enhancing IoT Security With Trust Management Using Ensemble XGBoost and AdaBoost Techniques

KAMRAN AHMAD AWAN[1], IKRAM UD DIN[1], (Senior Member, IEEE), AHMAD ALMOGREN[2], (Senior Member, IEEE), BYUNG-SEO KIM[3], (Senior Member, IEEE), AND MOHSEN GUIZANI[4], (Fellow, IEEE)

[1]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]Department of Software and Communications Engineering, Hongik University, Sejong 30016, Republic of Korea
[4]Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence, Abu Dhabi, United Arab Emirates

Corresponding author: Byung-Seo Kim (jsnbs@hongik.ac.kr)

This work was supported in part by Culture, Sports and Tourism R&D Program through the Korea Creative Content Agency grant funded by the Ministry of Culture, Sports and Tourism in 2024(Project Name: Global Talent Training Program for Copyright Management Technology in Game Contents, Project Number: RS-2024-00396709, Contribution Rate: 50%); in part by the Strategic Networking and Development Program funded by the Ministry of Science and ICT through the National Research Foundation of Korea under Grant RS-2023-00277267; and in part by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number (RSP2024R184).

ABSTRACT As next-generation networking environments become increasingly complex and integral to the fabric of digital transformation as the traditional perimeter-based security model proves inadequate. The Zero Trust framework emerges as a critical solution to this challenge, advocating for a security model that assumes no implicit trust and requires verification at every step. The rapid growth of the Internet of Things (IoT) creates an environment of millions of interacting devices that radically transform today's digital environment. In such conditions, the problem of identifying malicious and compromised nodes among IoT devices becomes mandatory to maintain trustworthy environment. The main objective of this research is to implement an advanced trust management mechanism, with the main transformation on the framework of security within which IoT environments become workable. To overcome this, an approach based on intelligent ensemble learning is presented in this paper by formulating a dataset consists of IoT-23, N-BaIoT, Edge-IIoTset, and AutoTrust-IoTDS. This work is specialized by selecting a diversified combination of features from these datasets to construct an effective dataset that would further enhance inculcation of trust in the IoT networks. The study proposed two notable models, i.e., XGBoost with logistic regression and AdaBoost with decision tree to achieve the efficiency and scalability of the proposed models. The results shows significant improvement in the efficiency, and having both the mentioned models to offer a precision, recall and F1-score of 0.99 representing efficient mechanism in ensuring a secure and dependable IoT ecosystem.

INDEX TERMS Internet of Things, next-generation networking, trust management, zero trust, ensemble learning, security, privacy preservation, trustworthiness.

I. INTRODUCTION

The integration of the Internet of Things (IoT) into next-generation networks represents a significant evolution in digital infrastructure [1], offering unparalleled opportunities for innovation across various sectors [2]. This integration, as discussed by Sarker et al. [3] and Rejeb et al. [4], expands the functional capabilities of networks while also introducing a complex array of security challenges. As Pham et al. [5] have noted the seamless connectivity

The associate editor coordinating the review of this manuscript and approving it for publication was Maurizio Casoni.

provided by IoT devices and elaborated the issue of safeguarding against increasingly security threats [6]. This pervasiveness of IoT technologies has clearly emphasized the huge need for strong security mechanisms that do not allow any kind of breach compromising either data privacy or operational integrity [7]. This worry is also expressed by Singhai and Sushil [8] and Liu et al. [9]. The Zero Trust security model is emerging as a foundational strategy for enhancing the security stance of such networks [10]. Juma et al. [11] and Ahmid and Kazar [12] provides comprehensive analysis of these vulnerabilities, underscoring the necessity for a security approach that is both adaptive and resilient.

As an emerging technology, it changes radically in many fields, from smart homes to industrial automation [13]. The most important ones are related to matters of security and trustworthiness of devices [14]. As the scope broadens and greater complexity is added, IoT networks become much more vulnerable to security breaches [15], carried out by either compromised or malicious nodes [16]. In turn, they can cause IoT systems to lose their efficiency and reliability [17]. To address these vulnerabilities, robust mechanisms are required in order to be able detect and mitigate such potential security threats [18]. The proposed methodology advances the implementation of the Zero Trust security model through the integration of two ensemble learning algorithms. The selection of these algorithms is predicated on their demonstrated efficacy in managing the complexity and the multi-dimensional nature of data associated with next-generation network environments. This article provides the following innovative contributions to the field of IoT trust management as itemized below:

- The proposed methodology is distinguished by its integration of features from four diverse datasets—IoT-23, N-BaIoT, Edge-IIoTset, and AutoTrust-IoTDS.
- A significant advancement in our approach is the application of ensemble learning algorithms, namely XGBoost and AdaBoost. Notably, AdaBoost incorporates a decision tree base estimator, enhancing the predictive accuracy and efficiency of our models.
- We have implemented a rigorous training and testing regimen to ensure the models' practical applicability. The deployment of our trained models within a simulated IoT environment facilitates a realistic appraisal of their performance.

The Structure of rest of the article is as follows: Section II delves into the Related Work, offering a comprehensive review. Section III describes the Materials and Methods employed in this study. Section IV presents the implementation of XGBoost within our proposed methodology. Similarly, Section V explores the integration of AdaBoost into the proposed security framework. Section VI reports on the Experimental Simulation & Outcome, providing an analysis of the results. Finally, Section IX concludes the paper.

II. RELATED WORK

As the number of network-connected devices continues to increase, the domain of the IoT presents unparalleled opportunities alongside significant challenges. This section systematically examines the latest scholarly contributions to IoT security, with a focused analysis on the identification and mitigation of malicious and compromised nodes.

Ren et al. [19] analyze experimentally, a trustworthiness prediction-stack ensemble learning model for the fog services in case of an SDN-enabled IoMT. This QWS dataset was used while enrichment of some selected features were effected through the proposed Variable Feature Set. Liu et al. [20] put forward an ensemble-based method to estimate the trustworthiness of data within the IoT networks, considering the integrity of sensor data. Rezaei [21] The paper has attempted optimization in the detection of botnet in the IoT using an ensemble learning model. Aaqib et al. [22] presented the research that dealt with the problem statement that now stronger trust management has to be implemented in IoT systems, focusing on the weaknesses of the previous machine learning approaches in catching the dynamic behavior of IoT devices. Verma and Chandra [23] analysed the emerging security threats in the fog-IoT network based on reputation, such as DoS/DDoS and Sybil attacks. The main aim of this research is the proposition of the RepuTE Framework: a novel machine learning-centric approach specially designed to enhance trust and security in the fog-IoT environment.

From the literature reviewed on IoT security, the proposed approach provides a more generalized and comprehensive approach, in particular terms of its application scope and attack resilience. In comparison with studies focused on specific IoT contexts, such as fog computing by Ren et al. [19] or the fog-IoT milieu in the work of Verma and Chandra [23], our model is designed for the entire IoT ecosystem. This holistic approach enables it to address a wider range of vulnerabilities inherent in diverse IoT environments. Further, the approaches as in the studies by Rezaei [21] and Aaqib et al. [22] are designed to work with one kind of attack, such as botnet attacks and reputation-based attacks, respectively, while our approach is to make the system resilient to a far more generic kind of attack through advanced ensemble learning algorithms over a custom-tailored set of features from a number of datasets.

III. MATERIALS AND METHODS

This study proposed a methodological framework designed to operationalize the Zero Trust security model within next-generation networking environments, encompassing both traditional and IoT networks. The foundation of the proposed approach is the formulation and utilization of datasets that reflect the diversity and complexity of modern network environments, facilitating the training of models to discern and mitigate a wide range of security vulnerabilities. The application of ensemble learning algorithms, specifically XGBoost and AdaBoost with logistic regression as a base estimator is central to the proposed methodology.

A. OVERVIEW OF THE PROPOSED APPROACH

The practical application of the theoretical framework and algorithmic basis is presented in our developed comprehensive algorithm, as depicted in Algorithm 1. This algorithm provides a systematic delineation of the trust score computation process for each IoT node, marrying the ensemble learning models with our innovative trust estimation methodology.

Algorithm 1 Trust Score Calculation in IoT Nodes

Result: Trust score for each IoT node
initialization;
foreach *IoT node i* **do**
  Extract behavioral features B_i;
  Extract network features N_i;
  foreach *model* $k \in K$ **do**
    Compute model output $M_k(B_i, N_i)$;
    Assign weight w_k to model k;
  end
  Calculate $F_{ensemble}(B_i, N_i) = \sum_{k=1}^{K} w_k \cdot M_k(B_i, N_i)$;
  Retrieve historical trust score T_{prev_i};
  Calculate $H(T_{prev_i}) = \beta \cdot \log(1 + T_{prev_i})$;
  Compute final trust score
  $T_{score_i} = \alpha \cdot F_{ensemble}(B_i, N_i) + (1 - \alpha) \cdot H(T_{prev_i})$;
end
Optimize each model C_j in ensemble:
$\theta_j^* = \arg\min_{\theta_j} L(D; \theta_j)$;
Determine ensemble weights:
$\Lambda^* = \arg\min_{\Lambda} \sum_{i=1}^{N} \left(y_i - \sum_{j=1}^{J} \lambda_j \cdot C_j(x_i; \theta_j^*)\right)^2$;

1) THEORETICAL FRAMEWORK

In the proposed framework, the trustworthiness of an IoT node i is quantified by a trust score, T_{score_i}, which integrates both ensemble learning outcomes and historical trust assessments through the following formulation:

$$T_{score_i} = \alpha \cdot F_{ensemble}(B_i, N_i) + (1 - \alpha) \cdot H(T_{prev_i}) \quad (1)$$

The ensemble function, $F_{ensemble}(B_i, N_i)$, is mathematically constructed as an aggregation of weighted model outputs, reflecting the node's behavior and network interactions:

$$F_{ensemble}(B_i, N_i) = \frac{1}{K} \sum_{k=1}^{K} w_k M_k(B_i, N_i) \quad (2)$$

Here, $M_k(B_i, N_i)$ signifies the output of the k-th model in the ensemble, addressing distinct facets of node attributes with weight w_k, and K denotes the ensemble size. The function $H(T_{prev_i})$, representing the historical trust assessment, is detailed as an infinite series expansion to incorporate the effect of all previous trust scores on the current evaluation:

$$H(T_{prev_i}) = \sum_{n=1}^{\infty} \beta^{n-1} T_{prev_i}^n \quad (3)$$

In this expression, β acts as a discount factor for preceding trust scores, highlighting the diminishing influence of older assessments. The proposed approach also introduces an additional functions to encapsulate node reliability and security metrics. Firstly, a reliability index, R_i, is defined as:

$$R_i = \gamma \cdot \log(1 + e^{F_{reliability}(B_i, N_i)}) \quad (4)$$

where γ is a scaling constant, and $F_{reliability}$ is a function of the node's behavioral and network characteristics. Similarly, a security metric, S_i, is formulated to evaluate the node's security posture:

$$S_i = \delta \cdot \sqrt{F_{security}(B_i, N_i)} \quad (5)$$

with δ serving as a normalization constant, and $F_{security}$ summarizing the node's security features.

2) ALGORITHMIC BASIS

The foundation of the proposed methodology lies in formulating ensemble learning approaches. This formulation is encapsulated in a composite model, $E(x)$, designed to enhance threat detection and mitigation capabilities through the integration of base learners, described as follows:

$$E(x) = \sum_{j=1}^{J} \lambda_j \cdot C_j(x; \theta_j) \quad (6)$$

Here, $E(x)$ represents the ensemble output for an input x, with C_j indicating the j-th base learner, λ_j the corresponding weight, θ_j the learner's parameters, and J the ensemble size. The optimization of each base learner, C_j, revolves around finding the ideal parameter set θ_j^*, achieved through minimizing a defined loss function L:

$$\theta_j^* = \arg\min_{\theta_j} L(D; \theta_j) \quad (7)$$

where D signifies the training dataset. The determination of weights λ_j is an optimization problem aimed at reducing ensemble error:

$$\Lambda^* = \arg\min_{\Lambda} \sum_{i=1}^{N} (y_i - E(x_i))^2 \quad (8)$$

with $\Lambda = \{\lambda_1, \ldots, \lambda_J\}$ representing the weight set, y_i the true outcome for the i-th instance, and N the dataset size. To further refine the model, we introduce an adaptive learning rate η for dynamic adjustment of weights λ_j, integrating gradient descent for iterative optimization:

$$\lambda_j^{(t+1)} = \lambda_j^{(t)} - \eta \cdot \frac{\partial}{\partial \lambda_j} L\left(D; \Lambda^{(t)}\right) \quad (9)$$

Additionally, a regularization term $R(\Lambda)$ is incorporated to mitigate overfitting, leading to a revised weight optimization objective:

$$\Lambda^* = \arg\min_{\Lambda} \left\{ \sum_{i=1}^{N} (y_i - E(x_i))^2 + \rho R(\Lambda) \right\} \quad (10)$$

TABLE 1. Summary of datasets utilized in the study.

Dataset	Key Features
IoT-23	Malware and benign captures with labels, duration, and protocols.
N-BaIoT	Network data for intrusion detection; Features include traffic characteristics, IP, port, protocol.
Edge-IIoTset	Data from 7 layers of IIoT testbed; Various attack types including DoS/DDoS, Man in the middle, etc.
AutoTrust-IoTDS	Focuses on trust parameters like competence, cooperativeness, and honesty.

The summation $\sum_{i=1}^{N}(y_i - E(x_i))^2$, which calculates the squared error between the predicted output $E(x_i)$ of the ensemble model for the i-th input x_i and the true output y_i, across all N data points, indicating the model's accuracy; and $\rho R(\Lambda)$, a regularization term weighted by ρ, which penalizes complexity in the model to prevent overfitting by controlling the magnitude of the weights in Λ.

B. DATASET DESCRIPTION AND PREPARATION

The integrity and relevance of the datasets underpin the credibility and applicability of any study, particularly in the domain of IoT security, where the heterogeneity and volume of data play pivotal roles. The datasets, namely IoT-23 [24], N-BaIoT [25], Edge-IIoTset [26], and AutoTrust-IoTDS [27], encompass a broad spectrum of IoT scenarios, from home automation to industrial IoT configurations. The key characteristics of the datasets used are given in Table 1, and their relevance with our research goals is emphasized.

C. DATA PREPROCESSING AND FEATURE SELECTION

Data preprocessing plays a pivotal role in our approach, encompassing several critical steps: data cleaning, handling null values, normalization, and feature selection.

- Data Cleaning: Let D be the original dataset and D' the refined dataset. The data cleaning can be expressed mathematically as:

$$D' = \{d \in D \mid \text{isValid}(d)\} \tag{11}$$

- Handling Null Values: Let N_v denote a null value whereas the handling of null values is defined as:

$$N_v = \begin{cases} \text{median}(F), & \text{if isNumeric}(F) \\ \text{mode}(F), & \text{otherwise} \end{cases} \tag{12}$$

- Normalization Process: Normalization is crucial to ensure that the scale of the data does not bias the analysis. By bringing all features to a common scale, we eliminate discrepancies that could skew the trust evaluation process. For a data point x_i in a feature set X, normalization is performed as follows:

$$x_i^{norm} = \frac{x_i - \min(X)}{\max(X) - \min(X)} \tag{13}$$

where x_i^{norm} is the normalized value, and $\min(X)$ and $\max(X)$ are the minimum and maximum values in the feature set X, respectively.

- Feature Selection Process: After normalization, we employ a feature selection mechanism to identify the most significant features. Given a set of N features, the feature significance score $S(f_i)$ for each feature f_i is defined as:

$$S(f_i) = \sum_{j=1}^{M} w_j \cdot \text{Corr}(f_i, T_j) \tag{14}$$

where M is the number of trust parameters, w_j is the weight assigned to the j-th trust parameter T_j, and $\text{Corr}(f_i, T_j)$ is the correlation coefficient between feature f_i and trust parameter T_j. The features with the highest scores $S(f_i)$ are selected for model training.

IV. XGBoost IN PROPOSED METHODOLOGY

XGBoost comprises a series of decision trees constructed sequentially, where each tree aims to correct the errors made by the preceding one. By integrating XGBoost into the proposed security framework, we aim to enhance the detection and mitigation of potential threats, ensuring a higher degree of network integrity and reliability. The sequential correction process inherent in XGBoost allows for a refined analysis of IoT security data, facilitating a more accurate identification of vulnerabilities and threats within the network.

XGBoost reflects a strategic emphasis on precision and efficiency in predictive modeling significant for the dynamic and heterogeneous nature of IoT ecosystems. Mathematically, this can be expressed as shown by Equations 15 [28].

$$\mathcal{L}(\phi) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k), \tag{15}$$

where $\mathcal{L}(\phi)$ represents the overall loss function, l is a differentiable convex loss function that measures the discrepancy between the predicted outcome $\hat{y}_i$ and the true value y_i, and Ω symbolizes the regularization term, which penalizes the complexity of the model. XGBoost improves upon traditional gradient boosting by introducing a regularization term $\Omega(f_k)$ [29], which mitigates overfitting. This term is formally expressed as:

$$\Omega(f_k) = \gamma T + \frac{1}{2}\lambda\|\omega\|^2, \tag{16}$$

where T is the number of leaves in the tree, ω represents the scores on the leaves, and γ and λ are parameters that control the tree's complexity.

A. XGBoost IN CENTRALIZED IoT TRUST SECURITY

The employment of XGBoost within a centralized IoT framework significantly enhances the architecture's security mechanisms. Centralization allows for a holistic view of network interactions, creating a fertile ground for XGBoost's

Algorithm 2 Centralized XGBoost for IoT Trust Management

Result: Predictive Model for Centralized IoT Trust Management
Input: Aggregated dataset from centralized IoT network, Learning rate η, Regularization parameters γ, λ
Output: Trained XGBoost model $F_{centralized}(x)$

Initialize $F_{centralized}(x) = 0$
for $t \leftarrow 1$ **to** T **do**
  Fit a logistic regression model $h_t(x)$ to minimize $\mathcal{L}_{centralized}(\phi)$
  Compute $\Omega(h_t) = \gamma T + \frac{1}{2}\lambda\|\omega\|^2$
  Update $F_{centralized}(x) \leftarrow F_{centralized}(x) + \eta h_t(x)$
  Update weights for next iteration
    - T is the number of leaves in the tree
    - ω represents the scores on the leaves
    - γ and λ are hyperparameters controlling model complexity
  Update the model:
  $F_{centralized}(x) \leftarrow F_{centralized}(x) + \eta f_t(x)$, where:
    - η is the learning rate, controlling the contribution of each tree
  Update instance weights for the next iteration using the gradient descent method
end
return $F_{centralized}(x)$

algorithmic prowess. The workflow of the centralized IoT trust management is shown by Algorithm 2.

The model's effectiveness is rooted in its optimization process, governed by the objective function $\mathcal{L}_{centralized}(\phi)$, which is a balance between predictive accuracy and model simplicity:

$$\mathcal{L}_{centralized}(\phi) = \sum_{i=1}^{n} l(y_i, \hat{y}_i^{(central)}) + \lambda \sum_{k=1}^{K} \Omega(f_k), \quad (17)$$

where $\hat{y}_i^{(central)}$ indicates the centralized prediction for the i-th data point, with λ moderating the regularization impact. The regularization component $\Omega(f_k)$ is articulated as:

$$\Omega(f_k) = \gamma T + \frac{1}{2}\lambda\|\omega\|^2, \quad (18)$$

Emphasizing model complexity control through T, the count of decision nodes, and ω, the vector of leaf weights in the k-th tree. The iterative refinement mechanism, a hallmark of gradient boosting, is encapsulated as:

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + \eta f_t(x_i), \quad (19)$$

which delineates the prediction adjustment at iteration t by incorporating the output $f_t(x_i)$ of the newly added tree, modulated by a learning rate η.

Algorithm 3 Decentralized XGBoost for IoT Node Trust Management

Result: Predictive Models for Decentralized IoT Nodes
Input: Local dataset for each IoT node, Learning rate η, Regularization parameters γ, λ
Output: Set of trained XGBoost models $\{F_{decentralized,j}(x)\}$ for each node j

for *each node* j **do**
  Initialize $F_{decentralized,j}(x) = 0$
  for $t \leftarrow 1$ **to** T_j **do**
    Fit a logistic regression model $h_{tj}(x)$ to minimize $\mathcal{L}_{decentralized}(\phi_j)$
    Compute $\Omega(h_{kj}) = \gamma T_j + \frac{1}{2}\lambda\|\omega_j\|^2$
    Update $F_{decentralized,j}(x) \leftarrow F_{decentralized,j}(x) + \eta h_{tj}(x)$
    Update weights for next iteration
  end
  return $F_{decentralized,j}(x)$
end

B. XGBoost IN DECENTRALIZED IoT TRUST MANAGEMENT

The application of XGBoost in a decentralized IoT framework presents unique challenges and opportunities. This decentralized approach requires a tailored adaptation of the XGBoost algorithm to effectively manage trust in a distributed manner. The implementation and workflow of the XGBoost in decentralized is illustrated in Algorithm 3.

In a decentralized setting, the XGBoost algorithm is implemented at each node, relying on locally available data for training and prediction. The objective function for a decentralized node can be expressed as:

$$\mathcal{L}_{decentralized}(\phi_j) = \sum_{i=1}^{n_j} l(y_{ij}, \hat{y}_{ij}^{(decentral)}) + \lambda \sum_{k=1}^{K_j} \Omega(h_{kj}), \quad (20)$$

where ϕ_j represents the parameters for node j, n_j is the number of samples at node j, $\hat{y}_{ij}^{(decentral)}$ is the predicted outcome for sample i at node j, and K_j denotes the number of logistic regression models at node j. Each node in the decentralized network trains its XGBoost model using local data. The logistic regression models are tuned and applied based on patterns in the data and potential security threats relevant to that node. The boosting mechanism, for each node, is mathematically formulated as:

$$\hat{y}_{ij}^{(t)} = \hat{y}_{ij}^{(t-1)} + \eta h_{tj}(x_{ij}), \quad (21)$$

where $\hat{y}_{ij}^{(t)}$ is the prediction for sample i at iteration t for node j, and $h_{tj}(x_{ij})$ represents the output of the new logistic regression model added at iteration t for node j. Under the decentralized paradigm, every node is able to independently decide on its current trust model and update it.

V. AdaBoost IN THE PROPOSED METHODOLOGY

AdaBoost is used in our proposed methodology for securing IoT environments. The basic principle of AdaBoost is working on the sequential technique of adding simple classifiers to an ensemble such that every coming one corrects the errors of its predecessor.

Let $D_t(i)$ be the weight assigned to each training example i at iteration t, with initial weights $D_1(i) = \frac{1}{N}$, where N is the total number of training examples. At each iteration, a weak classifier $h_t(x)$ is trained on the weighted samples. The error ϵ_t of $h_t(x)$ is calculated as:

$$\epsilon_t = \frac{\sum_{i=1}^{N} D_t(i) \cdot \mathbb{I}(y_i \neq h_t(x_i))}{\sum_{i=1}^{N} D_t(i)}, \tag{22}$$

where $\mathbb{I}(\cdot)$ is an indicator function that equals 1 when $y_i \neq h_t(x_i)$ (i.e., the prediction is incorrect) and 0 otherwise. The weight of each classifier in the final ensemble, α_t, is then determined by:

$$\alpha_t = \frac{1}{2} \ln \left(\frac{1 - \epsilon_t}{\epsilon_t} \right). \tag{23}$$

Subsequently, the weights for the next iteration are updated as:

$$D_{t+1}(i) = \frac{D_t(i) \cdot \exp(-\alpha_t \cdot y_i \cdot h_t(x_i))}{Z_t}, \tag{24}$$

where Z_t is a normalization factor to ensure that D_{t+1} is a probability distribution. Thus, AdaBoost is well suited to the work of identifying fairly subtle and complex patterns of malicious activities within the context of IoT security.

A. IMPLEMENTATION OF AdaBoost IN A CENTRALIZED IoT FRAMEWORK

In a centralized IoT environment, the AdaBoost algorithm is particularly poised to exploit the big collection of data available to the central authority. As shown in Algorithm 4, the classifiers are trained and they update adaptively the instance weights whereas the workflow is depicted by Figure 1.

The AdaBoost model, in this centralized context, can be mathematically expressed and elaborated as follows:

$$F_{centralized}(x) = \sum_{t=1}^{T} \alpha_t h_t(x), \tag{25}$$

where $h_t(x)$ denotes the weak classifiers, α_t their corresponding weights, and T the total number of classifiers. Each classifier $h_t(x)$ is a function that maps input features x to a predicted output, and α_t signifies the weight of classifier t in the final decision-making process. The weight α_t of each classifier is calculated based on its performance, with more accurate classifiers receiving higher weights. The weight for classifier t is given by:

$$\alpha_t = \frac{1}{2} \ln \left(\frac{1 - \epsilon_t}{\epsilon_t} \right), \tag{26}$$

Algorithm 4 AdaBoost for Centralized IoT Framework

Data: Training set $\mathcal{T} = \{(x_i, y_i)\}_{i=1}^{N}$, Number of classifiers T

Result: Final strong classifier $F_{centralized}(x)$

Initialize weights $D_1(i) = \frac{1}{N}, \forall i$;

for $t = 1$ **to** T **do**

  Train weak classifier $h_t(x)$ with weights $D_t(i)$;

  Calculate error $\epsilon_t = \frac{\sum_{i=1}^{N} D_t(i) \cdot \mathbb{I}(y_i \neq h_t(x_i))}{\sum_{i=1}^{N} D_t(i)}$, where:

  - ϵ_t is the weighted error rate of the weak classifier $h_t(x)$.

  Compute classifier weight $\alpha_t = \frac{1}{2} \ln \left(\frac{1-\epsilon_t}{\epsilon_t} \right)$, where:

  - α_t is the weight assigned to the weak classifier based on its accuracy.

  Update weights $D_{t+1}(i) = \frac{D_t(i) \cdot \exp(-\alpha_t \cdot y_i \cdot h_t(x_i))}{Z_t}$, where:

  - Z_t is a normalization factor to ensure $D_{t+1}(i)$ forms a probability distribution.

  Normalize $D_{t+1}(i)$ to ensure it forms a probability distribution;

Combine weak classifiers $F_{centralized}(x) = \sum_{t=1}^{T} \alpha_t h_t(x)$;

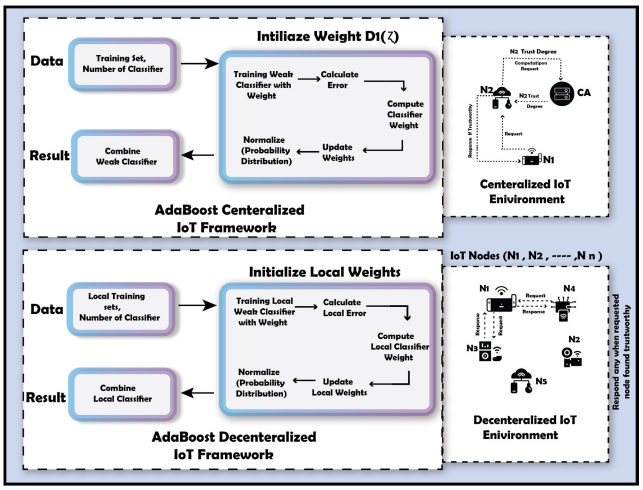


FIGURE 1. The implementation workflow of AdaBoost in the IoT environment.

where ϵ_t is the error rate of classifier t. It is computed as the proportion of misclassified instances, weighted by their importance in the dataset. After training each classifier, the weights of the training instances are updated to focus more on the misclassified instances. The updated weight of instance i for the next classifier $t + 1$ is calculated as:

$$D_{t+1}(i) = \frac{D_t(i) \cdot \exp(-\alpha_t \cdot y_i \cdot h_t(x_i))}{Z_t}, \tag{27}$$

where $D_t(i)$ is the weight of instance i for classifier t, y_i is the true label of instance i, $h_t(x_i)$ is the prediction of classifier t for instance i, and Z_t is a normalization factor ensuring that D_{t+1} forms a valid probability distribution.

Algorithm 5 AdaBoost for Decentralized Trust Management

Data: Local training sets $\mathcal{T}_j = \{(x_{ij}, y_{ij})\}$ for each node j, Number of classifiers T_j per node

Result: Set of strong classifiers $\{F_{decentralized,j}(x)\}$ for all nodes

foreach *node* j **do**

  Initialize local weights $D_{1j}(i) = \frac{1}{N_j}, \forall i \in \mathcal{T}_j$;

  for $t = 1$ **to** T_j **do**

    Train local weak classifier $h_{tj}(x)$ with weights $D_{tj}(i)$;

    Calculate local error $\epsilon_{tj} = \frac{\sum_{i \in \mathcal{T}_j} D_{tj}(i) \cdot \mathbb{I}(y_{ij} \neq h_{tj}(x_{ij}))}{\sum_{i \in \mathcal{T}_j} D_{tj}(i)}$, where:

    - ϵ_{tj} is the weighted error rate of the weak classifier $h_{tj}(x)$.

    Compute local classifier weight $\alpha_{tj} = \frac{1}{2} \ln\left(\frac{1-\epsilon_{tj}}{\epsilon_{tj}}\right)$, where:

    - α_{tj} is the weight assigned to the weak classifier

    Update local weights $D_{t+1,j}(i) = \frac{D_{tj}(i) \cdot \exp(-\alpha_{tj} \cdot y_{ij} \cdot h_{tj}(x_{ij}))}{Z_{tj}}$, where:

    - Z_{tj} is a normalization factor

    Normalize $D_{t+1,j}(i)$ to ensure it forms a probability distribution;

  Combine local classifiers $F_{decentralized,j}(x) = \sum_{t=1}^{T_j} \alpha_{tj} h_{tj}(x)$;

B. AdaBoost IN DECENTRALIZED TRUST MANAGEMENT

Application of AdaBoost to IoT security is decentralised that individual nodes in the systems make decisions in consideration of their local data. The learning of the AdaBoost is shown by Algorithm 5 where at each node of the network, a weak classifier is trained at each new iteration. Calculation of the weights of classifiers and subsequent updates in the AdaBoost methodology are adapted in a decentralized context to ensure each node gives an effective response to its own security environment.

In a decentralized setting, each node j independently trains its set of weak classifiers $h_{tj}(x)$. The model for each node is represented as:

$$F_{decentralized,j}(x) = \sum_{t=1}^{T_j} \alpha_{tj} h_{tj}(x), \tag{28}$$

where T_j denotes the number of classifiers at node j, and α_{tj} signifies the weight of the t-th classifier at node j. Each node's classifiers are trained on local data, enabling the model to adapt to the specific security. The weight α_{tj} of each classifier is computed similarly to the centralized approach, yet it is crucial to account for the localized nature of the data. The error rate ϵ_{tj} of each classifier is specific to node j and calculated based on the node's dataset. The weight for classifier t at node j is given by:

$$\alpha_{tj} = \frac{1}{2} \ln\left(\frac{1-\epsilon_{tj}}{\epsilon_{tj}}\right), \tag{29}$$

where ϵ_{tj} is the error rate of classifier t at node j. Post-classification, the weights are updated of those instances which were misclassified, the entire focus is to train the next classifier on these data. This update is important for making the model evolve continuously from being weak to stronger and highly adaptive.

TABLE 2. Parameters and protocols in IoT network replication.

Component	Specification
Node Configuration	IoT devices with ARM Cortex processors
Communication Protocol	IPv4/IPv6, MQTT, CoAP
Security Settings	TLS/SSL encryption, IPSec for security
Transmission Frequency	Every 30 seconds
Sensor Types	Temperature, Humidity, Motion sensors
Actuator Types	LEDs, Motors, Relays
Network Topology	Mesh topology with Zigbee protocol
Data Encryption	AES-256 for data encryption
Anonymization	Data masking and pseudonymization
Scalability Features	Dynamic node addition/removal capability
Fault Tolerance	Redundant paths and data replication

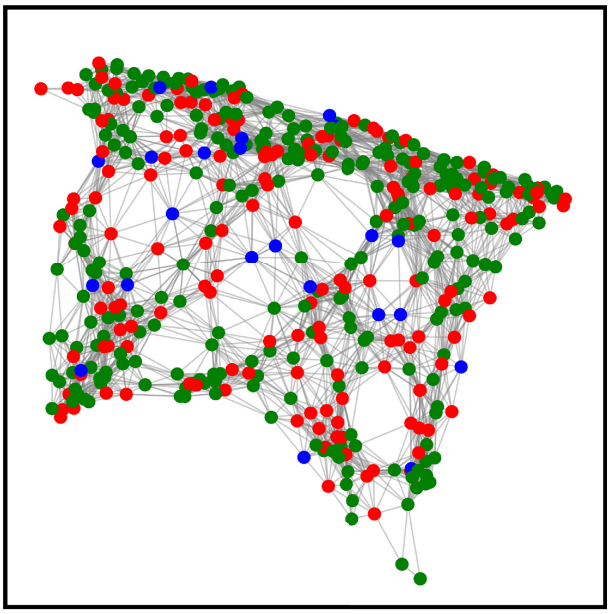
VI. EXPERIMENTAL SIMULATION AND OUTCOME

This section demonstrates the applicability and effectiveness of our proposed trust management mechanism in IoT environments. We employed a comprehensive simulation environment utilizing Jupyter Notebook for both training and testing phases of our dataset. In the proposed approach, we look at centralized and distributed implementations of trust, using both the XGBoost and AdaBoost algorithms in order to evaluate performance under these two paradadigms. Additionally, we conducted a comparative analysis of our approach against established models in the literature, specifically SELM [19], ETSM [20], ELTB [21], BTAMC [22], and RepuTE [23].

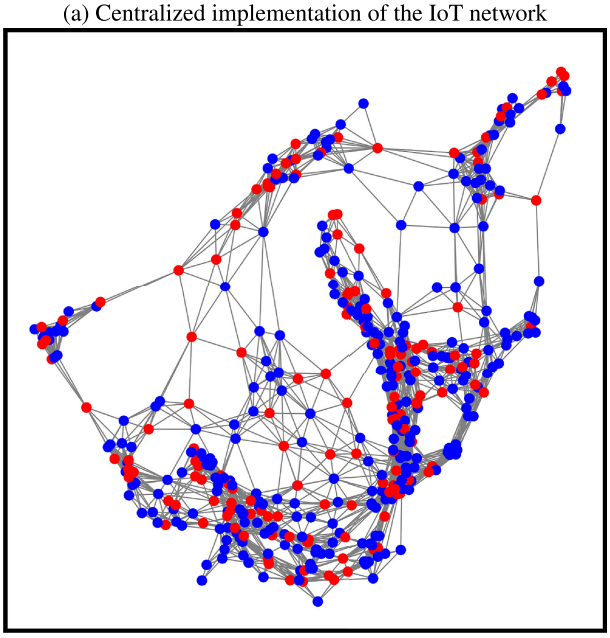
A. DEPLOYMENT AND INTEGRATION IN IoT SYSTEMS

We have integrated the proposed ensemble learning methods XGBoost and AdaBoost into IoT systems is one of the most important steps in validating the applicability in reality. This section details how an IoT network is built and how our models have been deployed in a centralized trust management architecture. The main configurations that, collectively, make a full setup of our IoT network in the simulation are presented in the Table 2.

As depicted in Figure 2, our IoT network is made up of 450 nodes, each represented by a corresponding IoT device. The central node collects data from all other nodes and applies the trained models for XGBoost and AdaBoost to compute trust scores as depicted in Figure 2a. The centralized system simulates scenarios where a central server or gateway manages trust across the IoT network. In contrast, in the



(a) Centralized implementation of the IoT network



(b) Decentralized implementation of the IoT network.

FIGURE 2. Implementation of IoT network for simulation-based algorithm evaluation.

decentralized way, as depicted by Figure 2b, every IoT node computes its own trust score independently using the same ensemble models.

The data from IoT devices flows in the network through to the trust assessment models. The centralized approach sends data to the central node for routing, whereas in the decentralized approach, data is computed and processed locally at each node. Then it analyzes the behavior of each node and also calculates a trust score by using the ensemble models. This is based upon various parameters, such as consistency in data, historical trust, and interactions by the nodes. Key metrics include detection accuracy, false positive rates, and system latency. Dealing with scalability of the network in the case of 450 nodes in the IoT model is a big issue, especially in decentralized approaches.

TABLE 3. Adaptive boosting classification report using base-estimator of decision tree.

	Precision	Recall	F1-Score
0	0.99	0.99	0.99
1	0.99	0.99	0.99
Accuracy			0.99
Macro Avg	0.99	0.99	0.99
Weighted Avg	0.99	0.99	0.99

TABLE 4. XGBoost classification report.

	Precision	Recall	F1-Score	Support
0	0.98	1.00	0.99	21,163
1	1.00	0.98	0.99	23,837
Accuracy			0.99	45,000
Macro Avg	0.99	0.99	0.99	45,000
Weighted Avg	0.99	0.99	0.99	45,000

B. ACCURACY, PRECISION, RECALL, AND F1-SCORE

The AdaBoost model exhibited remarkable performance across all metrics. As shown in the classification report (see Table 3), the model achieved an accuracy, precision, recall, and F1-score of 0.99 for both classes (0 and 1), indicating an almost perfect ability to classify nodes accurately. The macro and weighted averages of 0.99 for precision, recall, and F1-score further underscore the model's consistent performance across different classes.

Similarly, the XGBoost model demonstrated exceptional performance. As detailed in the classification report (see Table 4), it achieved precision scores of 0.98 and 1.00 for classes 0 and 1, respectively, and recall scores of 1.00 and 0.98. The F1-scores for both classes were 0.99, mirroring the high level of model accuracy at 0.99. The model's support of 21,163 and 23,837 for classes 0 and 1, respectively, illustrates its robustness in handling a significant volume of data points.

Through the comparisons of the models, it is clear that the models provide high-level accurate and consistent performance in recognizing the existence of both trusted and untrusted nodes within the IoT environment. The marginal difference of precision and recall of the models shows strong and exact levels of the models for classification.

C. COMPARATIVE ANALYSIS WITH EXISTING APPROACHES

This section presents a comparative analysis of the proposed XGBoost model against state-of-the-art approaches:

TABLE 5. Classification reports of comparative models.

Model		Precision	Recall	F1-Score
SELM [19]	0	0.95	0.96	0.95
	1	0.94	0.97	0.95
ETSM [20]	0	0.97	0.94	0.95
	1	0.96	0.98	0.97
ELTB [21]	0	0.96	0.97	0.96
	1	0.97	0.95	0.96
BTAMC [22]	0	0.98	0.95	0.96
	1	0.97	0.99	0.98
RepuTE [23]	0	0.97	0.98	0.97
	1	0.98	0.96	0.97

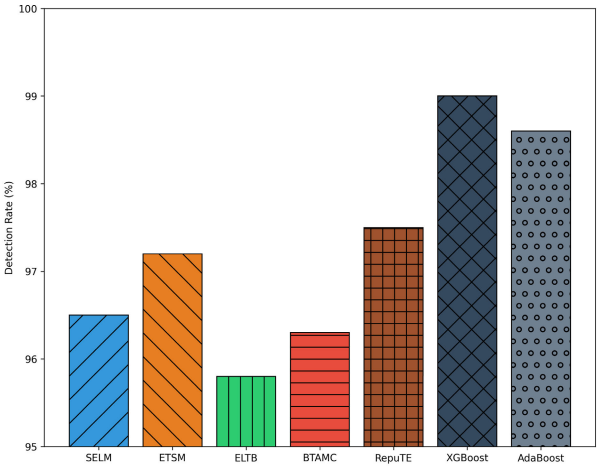


FIGURE 3. The detection rate performance analysis.

SELM [19], ETSM [20], ELTB [21], BTAMC [22], and RepuTE [23]. Table 5 provides a comprehensive overview of the classification reports for the comparative models:

The analysis of these models shows that SELM [19] shows strong precision and recall, indicating its efficiency in accurately detecting various threat. ETSM [20] also maintains high precision. ELTB [21] and BTAMC [22] also demonstrate a significant precision and recall, indicating their robustness in diverse scenarios. Notably, RepuTE [23] achieves the highest F1-score, highlighting its superior balance in precision and recall.

The evaluation of our proposed models in the IoT environment shows a noteworthy performance, particularly in terms of accuracy. The XGBoost model shows an overall accuracy of 0.99% that outperforms the comparative models i.e., SELM (0.95%), ETSM (0.96%), ELTB (0.96%), BTAMC (0.97%), and RepuTE (0.97%). Similarly, the AdaBoost model, with its precision, recall, and F1-score all at 0.99%.

VII. PERFORMANCE ANALYSIS IN DECENTRALIZED TRUST IOT

We have evaluated the effectiveness of our XGBoost and AdaBoost models in detecting malicious activities in a decentralized IoT environment with 450 nodes and a mix of 35% of malicious to 65% of trustworthy nodes.

A. DETECTION RATE EVALUATION

The XGBoost model, with the use of a decentralized IoT setup, demonstrated exemplary detection rates in this matter. It managed to detect 99% of the malicious nodes, and this shows sensitivity and accuracy in these threats' detection. The AdaBoost model, through a weak ensemble of learners to build up a strong learner, showed almost a similar performance to the model with XGBoost. It shows a detection rate of 98.6% for the malicious nodes which shows almost similar efficiency shown by the XGBoost model, as shown in Figure 3. This section extends our analysis on decentralized IoT environments and delves deeper into the comparison of the detection rates with SELM, ETSM, ELTB, BTAMC, and RepuTE using our models XGBoost and AdaBoost. On the other hand, SELM could achieve a detection rate of 96.5%, while ETSM derived 97.2%. The performance of ELTB was noted at 95.8% and BTAMC showed a rate of 96.3%. The most recent among these, RepuTE, showed the rate of 97.5%. Our XGBoost model showed an impressive rate of 99% and AdaBoost gave a closely approximate one—98.6%.

B. PERFORMANCE OUTCOMES AGAINST IoT COMMON ATTACKS

To evaluate the performance of the proposed models against IoT attacks, specifically, On-off, Good Mouthing, Bad Mouthing, and White Washing attacks. In evaluation the On-off attack, where attackers intermittently behave maliciously, the XGBoost model detected anomalies with an accuracy of 95.4%, while AdaBoost reported a precision of 94.7% (see Figure 4). The SELM model, in comparison, stood at 92.1%, ETSM at 93.3%, ELTB at 90.9%, BTAMC at 91.8%, and RepuTE at 93.7%. In Good Mouthing attack scenario, where malicious nodes consistently rate other bad nodes positively, the XGBoost model's effectiveness was marked at 96.8%. In contrast, AdaBoost's performance was slightly lower at 96.1%, as shown in Figure 5. SELM's response to this attack yielded an 89.7% success rate, ETSM at 91.2%, ELTB at 88.5%, BTAMC at 90.3%, and RepuTE at 92.4%.

The simulation related to Bad Mouthing attack is implemented wherein malicious nodes give negative feedback to good nodes, the proposed XGBoost model achieving a 97.5% detection rate, as shown in Figure 6. AdaBoost closely followed with 96.9%. SELM with 87.6% detection rate, ETSM at 88.8%, ELTB at 86.3%, BTAMC at 87.0%, and RepuTE at 89.5%. Lastly, for the White Washing attack, where attackers reset their bad history by rejoining the network, XGBoost and AdaBoost models reported detection

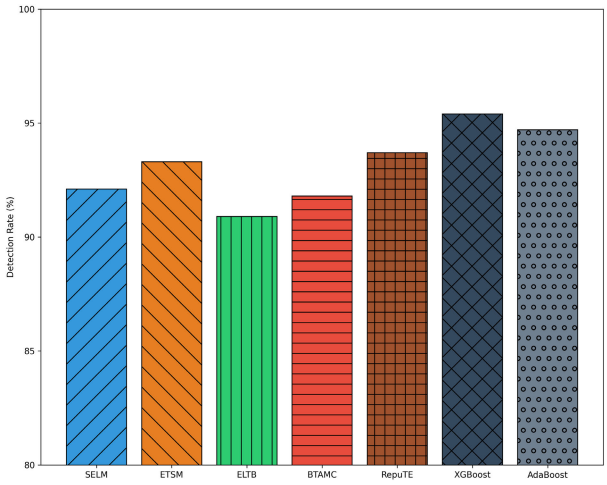


FIGURE 4. Comparative performance analysis of IoT security approaches against On-off attack.

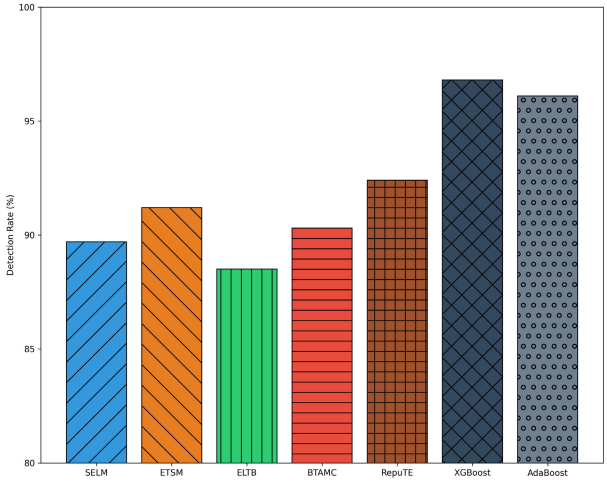


FIGURE 5. Comparative performance analysis of IoT security approaches against good mouthing attack.

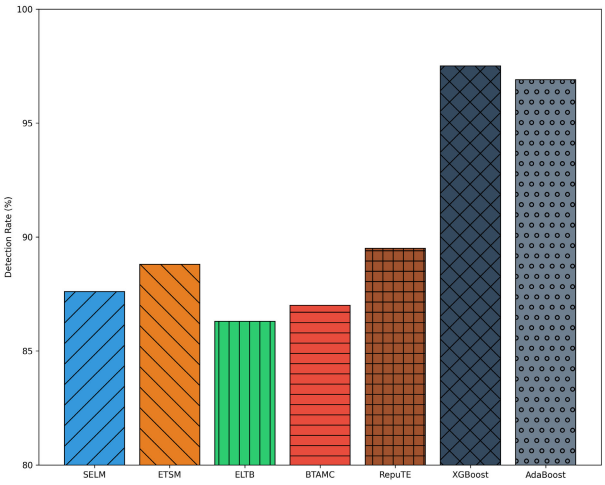


FIGURE 6. Comparative performance analysis of IoT security approaches against bad mouthing attack.

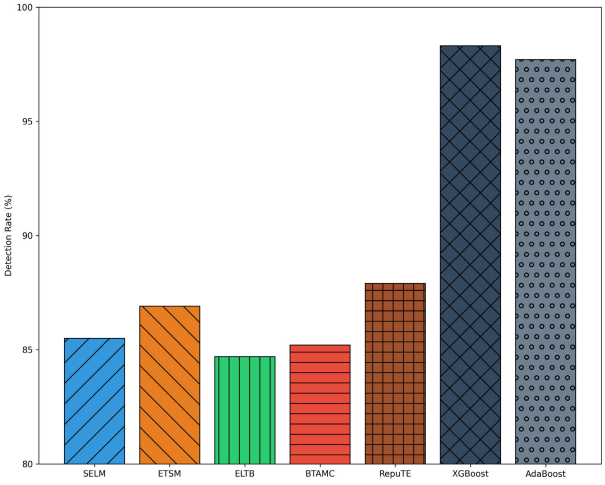


FIGURE 7. Comparative performance analysis of IoT security approaches against white washing attack.

rates of 98.3% and 97.7%, respectively (see Figure 7). SELM confronted this attack with an 85.5% detection rate, ETSM at 86.9%, ELTB at 84.7%, BTAMC at 85.2%, and RepuTE at 87.9%.

VIII. CENTRALIZED IMPLEMENTATION OF IOT ENVIRONMENT

Compared to the decentralized implementation, a centralized IoT environment postulates a single authoritative entity responsible for comprehensive management of IoT nodes. This implementation of this configuration is same with 450 nodes comprising of 35% malicious nodes and 65% trustworthy nodes.

A. DETECTION RATE EVALUATION IN CENTRALIZED IoT TRUST MANAGEMENT

This section evaluates the performance of the models XGBoost and AdaBoost in terms of the detection rate under such an environment. XGBoost, famous for its accuracy in distributed settings, has adapted surprisingly well to the centralized paradigm, with a detection rate of 99.5%, as shown in Figure 8. This slight increase over the decentralized environment underscores the capability of the model to benefit from centralized data aggregation, which tends to a more defined detection capability. The AdaBoost model has also exhibited an increase in the detection rate, which is found at 99.1%.

In this centralized framework, SELM displayed a detection rate of 96.8%, an incremental improvement from its decentralized equivalent. ETSM achieved a rate of 97.4%, showcasing its adaptability to centralized management. ELTB's performance was observed at 96.1%, while BTAMC exhibited a detection rate of 96.6%. RepuTE, adapting to the centralized structure, achieved a rate of 97.8%.

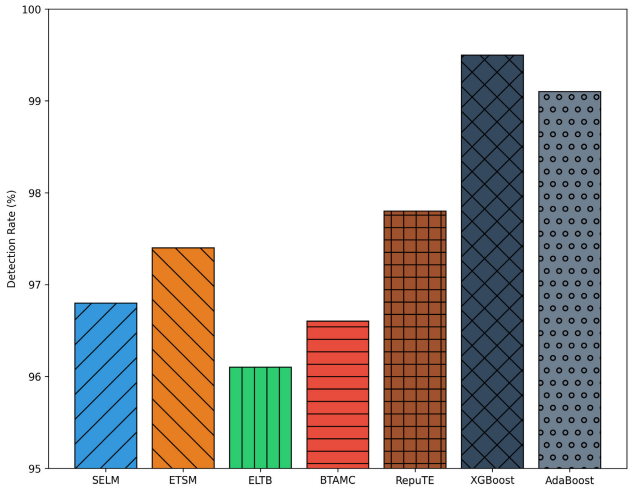


FIGURE 8. Detection rate of malicious nodes in centralized IoT environment.

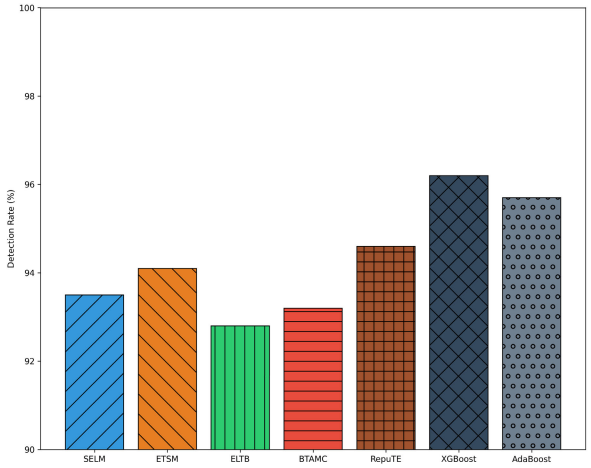


FIGURE 9. Comparative performance analysis of centralized IoT security approaches against on-off attack.

B. PERFORMANCE ANALYSIS AGAINST COMMON ATTACKS IN CENTRALIZED IoT TRUST MANAGEMENT

The performance of security algorithms against various attack vectors becomes a critical evaluation metric. Hence, this part is fully dedicated to the interpretation and demonstration of the efficacy of our proposed XGBoost and AdaBoost models in comparison with benchmark models of SELM, ETSM, ELTB, BTAMC, and RepuTE under a centralized system against prevalent IoT attacks.

In the evaluation against On-off attack, the XGBoost model demonstrated an exceptional detection rate of 96.2% (see Figure 9), while AdaBoost achieved 95.7%. Among the other models, SELM recorded a detection rate of 93.5%, ETSM at 94.1%, ELTB at 92.8%, BTAMC at 93.2%, and RepuTE at 94.6%. During the Good Mouthing attack, XGBoost excelled with a detection rate of 97.3%. AdaBoost followed closely with 96.9%. The SELM model detected

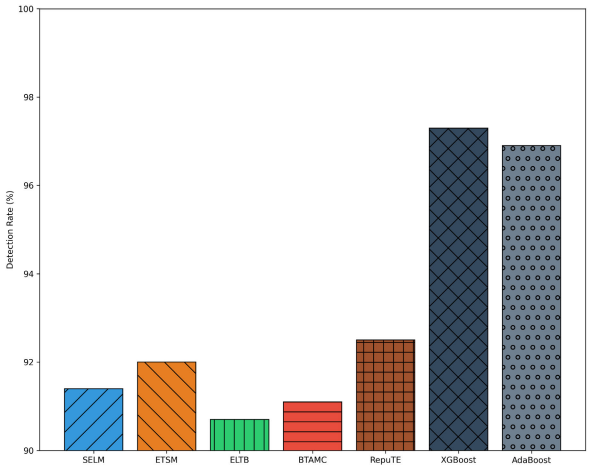


FIGURE 10. Comparative performance analysis of centralized IoT security approaches against good mouthing attack.

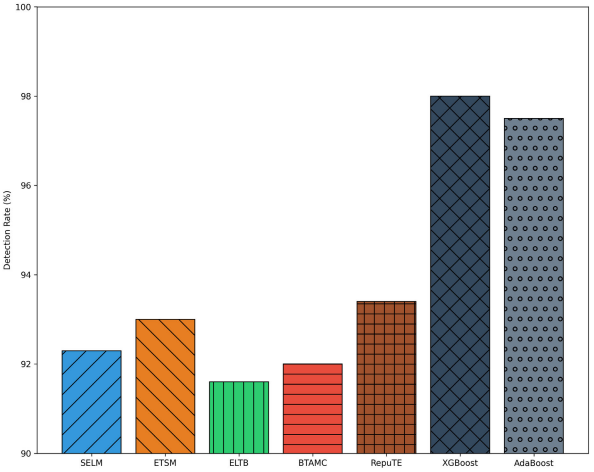


FIGURE 11. Comparative performance analysis of centralized IoT security approaches against bad mouthing attack.

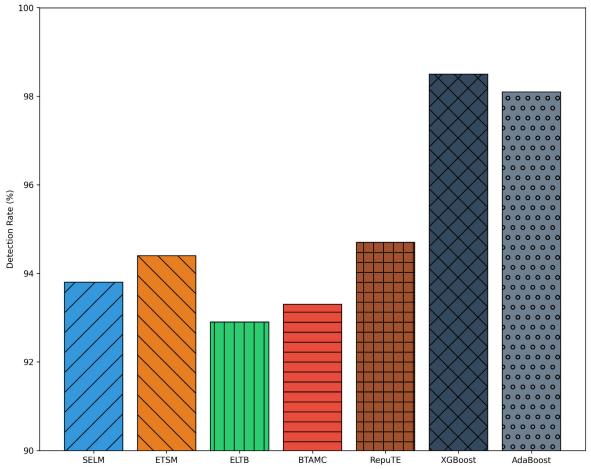


FIGURE 12. Comparative performance analysis of centralized IoT security approaches against white washing attacks.

this attack with an efficacy of 91.4%, ETSM at 92.0%, ELTB at 90.7%, BTAMC at 91.1%, and RepuTE at 92.5%

(see Figure 10). For the Bad Mouthing attack, XGBoost and AdaBoost showcased detection rates of 98.0% and 97.5%, respectively. In comparison, SELM achieved a rate of 92.3%, ETSM at 93.0%, ELTB at 91.6%, BTAMC at 92.0%, and RepuTE at 93.4%, as shown in Figure 11. Against the White Washing attack, the XGBoost model maintain a detection rate of 98.5%, and AdaBoost reported 98.1%, as represented by Figure 12. The other models performed as follows: SELM at 93.8%, ETSM at 94.4%, ELTB at 92.9%, BTAMC at 93.3%, and RepuTE at 94.7%.

IX. CONCLUSION

This research mainly focusing to enhance the management of trust in IoT environments by adopting advanced ensemble learning techniques. In our proposed work, we have designed and implemented XGBoost and AdaBoost models to cater to specific security problems in IoT networks. These models are developed to really detect as well as adaptively respond to a variety of malicious activities. More generally, for both centralized as well as decentralized IoT, the performances of the XGBoost and AdaBoost models had performances for detection of the existence of bad nodes which were beyond the standard benchmarks. The proposed models were constantly better compared to other prevailing systems in popular IoT attacks, for instance, On-off, Good Mouthing, Bad Mouthing, and White Washing attacks. Comparative analysis of the estimated models SELM, ETSM, ELTB, BTAMC, and RepuTE allows one to provide evidence of superiority in proposed solutions. This both points out the potential and limitations of current IoT security strategies by displaying clear nuances in detection rates and adaptability across various attack scenarios. The next step in the advancement of trust management for IoT is integrating such models in real IoT deployments, together with an examination of their scalability and efficiency in various, dynamic environments. As an significant step towards real environment verification, it is important to conduct pilot studies in controlled IoT environments to identify and mitigate integration challenges.

REFERENCES

[1] G. Rathee, R. Iqbal, C. A. Kerrache, and H. Song, "TrustNextGen: Security aspects of trustworthy next-generation industrial Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 15, pp. 25568–25576, Aug. 2024.

[2] A. Yazdinejad, A. Dehghantanha, G. Srivastava, H. Karimipour, and R. M. Parizi, "Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things," *J. Syst. Archit.*, vol. 148, Mar. 2024, Art. no. 103088.

[3] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023.

[4] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100721.

[5] Q.-V. Pham, M. Zeng, O. A. Dobre, Z. Ding, and L. Song, "Guest editorial special issue on aerial computing for the Internet of Things (IoT)," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 5623–5625, Apr. 2023.

[6] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang, and X.-Z. Gao, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet Things J.*, early access, Mar. 1, 2024, doi: 10.1109/JIOT.2024.3372518.

[7] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Federated quantum-based privacy-preserving threat detection model for consumer Internet of Things," *IEEE Trans. Consum. Electron.*, early access, Mar. 14, 2024, doi: 10.1109/TCE.2024.3377550.

[8] R. Singhai and R. Sushil, "An investigation of various security and privacy issues in Internet of Things," *Mater. Today, Proc.*, vol. 80, pp. 3393–3397, Jan. 2023.

[9] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on blockchain-based trust management for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 5898–5922, Apr. 2023.

[10] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6G security," *IEEE Netw.*, vol. 38, no. 4, pp. 224–232, Jul. 2024.

[11] M. Juma, F. Alattar, and B. Touqan, "Securing big data integrity for industrial IoT in smart manufacturing based on the trusted consortium blockchain (TCB)," *IoT*, vol. 4, no. 1, pp. 27–55, Feb. 2023.

[12] M. Ahmid and O. Kazar, "A comprehensive review of the Internet of Things security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, Jul. 2023.

[13] B. Babayigit and M. Abubaker, "Industrial Internet of Things: A review of improvements over traditional SCADA systems for industrial automation," *IEEE Syst. J.*, vol. 18, no. 1, pp. 120–133, Mar. 2023.

[14] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. de Ree, G. Mantas, J. Rodriguez, W. Aman, and S. Al-Kuwari, "Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 347–388, 1st Quart., 2024.

[15] H. Du, J. Wang, D. Niyato, J. Kang, Z. Xiong, M. Guizani, and D. I. Kim, "Rethinking wireless communication security in semantic Internet of Things," *IEEE Wireless Commun.*, vol. 30, no. 3, pp. 36–43, Jun. 2023.

[16] M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran, and N. Javaid, "Malicious node detection using machine learning and distributed data storage using blockchain in WSNs," *IEEE Access*, vol. 11, pp. 6106–6121, 2023.

[17] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1775–1807, 3rd Quart., 2023.

[18] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," *IEEE Access*, vol. 11, pp. 28934–28954, 2023.

[19] J. Ren, H. Wan, C. Zhu, and T. Qin, "Stacking ensemble learning with heterogeneous models and selected feature subset for prediction of service trust in Internet of Medical Things," *IET Inf. Secur.*, vol. 17, no. 2, pp. 269–288, Mar. 2023.

[20] J. Liu, S. Adams, and P. A. Beling, "An ensemble trust scoring method for Internet of Things sensor networks," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.

[21] A. Rezaei, "Using ensemble learning technique for detecting botnet on IoT," *Social Netw. Comput. Sci.*, vol. 2, no. 3, p. 148, May 2021.

[22] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, "Behaviour-based trust assessment in the Internet of Things systems using multi-classifier ensemble learning and Dempster–Shafer fusion," *Available SSRN*, Oct. 2023, doi: 10.2139/ssrn.4612140.

[23] R. Verma and S. Chandra, "RepuTE: A soft voting ensemble learning framework for reputation-based attack detection in fog-IoT milieu," *Eng. Appl. Artif. Intell.*, vol. 118, Feb. 2023, Art. no. 105670.

[24] S. Garcia, A. Parmisano, and M. J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic," Zenodo, Version 1.0.0, 2020, doi: 10.5281/zenodo.4743746.

[25] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018.

[26] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.

[27] K. A. Awan, I. U. Din, A. Almogren, and J. J. P. C. Rodrigues, "AutoTrust: A privacy-enhanced trust-based intrusion detection approach for Internet of Smart Things," *Future Gener. Comput. Syst.*, vol. 137, pp. 288–301, Dec. 2022.

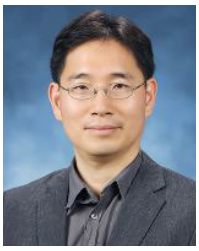
[28] R. A. Abbasi, N. Javaid, M. N. J. Ghuman, Z. A. Khan, S. Ur Rehman, and Amanullah, "Short term load forecasting using XGBoost," in *Web, Artificial Intelligence and Network Applications* (Advances in Intelligent Systems and Computing), vol. 927, L. Barolli, M. Takizawa, F. Xhafa, and T. Enokido, Eds., Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-15035-8_108.

[29] F. Xie, Z. Yin, A. Luo, and J. Yuan, "Prediction of distribution network line loss based on grey relation analysis and XGboost," in *Proc. IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng. (ICBAIE)*, Mar. 2021, pp. 279–284.

KAMRAN AHMAD AWAN received the B.S. and M.S. degrees in computer science from the Department of Information Technology, The University of Haripur, Pakistan, in 2015 and 2019, respectively, where he is currently pursuing the Ph.D. degree. His research interests include trust management in the Internet of Things, blockchain, security in metaverse, and information security.

IKRAM UD DIN (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM), in 2016. Currently, he is an Associate Professor with the Department of Information Technology, The University of Haripur. He has 15 years of teaching and research experience in different universities/organizations. His current research interests include traffic measurement and analysis for monitoring quality of service, mobility and cache management in information-centric networking, metaverse, and the Internet of Things. He also served as the IEEE UUM Student Branch Professional Chair.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is currently a Professor of the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. He is the Director of Cyber Security Chair, CCIS, KSU. Previously, he was the Vice Dean for the Development and Quality, CCIS. He was the Dean of the College of Computer and Information Sciences and the Head of the Academic Accreditation Council, Al-Yamamah University. His research interests include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.



BYUNG-SEO KIM (Senior Member, IEEE) received the B.S. degree in electrical engineering from Inha University, Inchon, South Korea, in 1998, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Yuguang Fang. From 1997 to 1999, he was with Motorola Korea Ltd., Paju, South Korea, as a Computer Integrated Manufacturing (CIM) Engineer with the Advanced Technology Research and Development (ATR&D). From January 2005 to August 2007, he was with Motorola Inc., Schaumburg Illinois, as a Senior Software Engineer in networks and enterprises. From 2012 to 2014, he was the Chairperson of the Department of Software and Communications Engineering, Hongik University, South Korea, where he is currently a Professor. His research focuses on Motorola Inc. designing protocol and network architecture of wireless broadband mission critical communications. His work has appeared in around 174 publications and 25 patents. His research interests include the design and development of efficient wireless/wired networks, including link-adaptable/cross-layer-based protocols, multi-protocol structures, wireless CCNs/NDNs, mobile edge computing, physical layer design for broadband PLC, and resource allocation algorithms for wireless networks. He also served as a member of Sejong-City Construction Review Committee and Ansan-City Design Advisory Board. He served as the General Chair for the 3rd IWWCN 2017, and a TPC Member for the IEEE VTC 2014-Spring, the EAI FUTURE 2016, and ICGHIT 2016–2019 conferences. He served as a Guest Editors for Special Issues of *International Journal of Distributed Sensor Networks* (SAGE), IEEE Access, *MDPI Sensors*, and *Journal of the Institute of Electrics and Information Engineers*. He is an Associative Editor of IEEE Access.

MOHSEN GUIZANI (Fellow, IEEE) received the B.S. (Hons.) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor with the Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, United Arab Emirates. He is a Senior Member of ACM.