RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt26329

Machine Learning-Based Risk-Adaptive Attribute- Based Access Control Framework for Secure IoT Networks

Rashmin Prajapati [a,*], Sweta S. Panchal [b], Neha Soni [c], Sandipkumar R. Panchal [b]

[a] Department of Computer Engineering, Dr. Subhash University, Junagadh - 362001, India
[b] Department of Electronics & Communication Engineering, Dr. Subhash University, Junagadh, India
[c] Department of Computer Engineering, Sardar Vallabhbhai Patel Institute of Technology, Vasad, India
* Corresponding Author Email: rashmin.1012@gmail.com
DOI: https://doi.org/10.54392/irjmt26329
Received: 10-02-2026; Revised: 10-05-2026; Accepted: 19-05-2026; Published: 30-05-2026

Abstract: Internet of Things (IoT) communication networks have been growing rapidly, which exposes security threats to the heterogeneity of the devices, changing circumstances, and changing attack patterns. Classical Role-Based Access Control (RBAC) and attribute-based access control (ABAC) models are not flexible and do not give real-time risk indicators and responsiveness to decision making. In this paper, a risk-adaptive attribute-based access control (RAd-ABAC) framework based on machine learning is proposed as a part of a secure IoT communication system. The model combines the modeling of subject, object, and environmental attribute with dynamic risk scoring performed by a supervised machine learning model. A ternary authorization scheme, Permit, Review, and Deny, is presented to enhance the decision granularity as well as be able to respond to borderline access requests better than binary authorization schemes. IoT23 and TON IoT benchmark datasets containing 45,000 samples converted into ABAC compatible feature vectors were used in the proposed framework evaluation. The experimental findings indicate that the proposed RAd-ABAC framework with a proposed accuracy of 94.6 percent, macro-average AUC of 0.97 and a false positive rate of 4.2. The false positive rate decreased by 8.3 percentage points, reaching 4.2%, which corresponds to a 66.4% relative reduction than the Static ABAC and is considered an absolute change of 8.3 and a relative change of 66.4. The scalability analysis also demonstrated near-linear scaling in processing performance of average latency of less than 5.4 ms per request. Results show that risk scoring using ML has the potential of enhancing the accuracy, flexibility, and reliability of authorization in distributed IoT communication systems.

Keywords: Attribute-Based Access Control (ABAC), Risk-Adaptive Access Control, Internet of Things (IoT), Machine Learning, Secure IoT Networks, Context-Aware Security, Zero Trust Architecture

1. Introduction

New and fast development of Internet of things (IoT) communication networks have altered the contemporary digital landscapes with massive connectivity of sensors, smart devices, wearable, industrial controllers, medical devices, and smart-city structures. They are used to monitor in real time, make decisions automatically and exchange data across several locations [1]. Yet, these very properties contribute to the popularity of IoT systems, which exacerbate the security risks as well. The IoT environments are extremely heterogeneous, resource-limited, decentralized, and context-dependent and are prone to unauthorized access, malicious communication, misuse of information, and adaptive cyberattacks [2-4].

Access control is a key component to the safety of IoT communication systems since it can decide if a device, user or service may access a certain resource or not within a certain situation. Conventional Role-Based Access Control (RBAC) is easy to administer and still lacks flexibility in terms of dynamic IoT settings where devices change their states, user activities, network, and situational risk on a continuous basis [5, 6]. To enhance flexibility, the principles of attribute-based Access Control (ABAC) allow applying subject, object, and environmental attributes when making authorization decisions [7, 8]. Traditional ABAC models are often rule-based and static. They all tend to lack real-time risk prediction, machine learning-driven behavioral modeling, and optimizing policy controls. Consequently, they cannot react to the fluctuating threat situations in the IoT communication networks [9].

Risk-Adaptive Access Control (RAdAC) and zero-trust methods aim at resolving these shortcomings with the introduction of contextual risk assessment and ongoing validation [10-11]. However, much of the current models continue to rely on manually-configured risk parameters, fixed thresholds or permit/deny decisions. Machine learning has permeated the IoT security space in intrusion detection, anomaly detection and authentication, but not in the authorization decision making of ABAC (But it has not yet been as well developed) [12, 13]. Specifically, current literature tends to lack the proposed combination of subject-object-environment attribute modeling, learned risk scoring and multi-state authorization integrated into a single IoT access-control framework. In order to fill this gap, this paper suggests a Risk-Adaptive Attribute-Based Access Control (RAd-ABAC) system based on machine learning to create a secure IoT communication network. The offered framework combines the use of ABAC-friendly attribute modelling with the use of controlled machine learning-based dynamic risk scoring. It also contributes a ternary authorization mechanism with Permit, Review, and Deny decisions. The Review state is meant to deal with uncertain or borderline requests which are not to be automatically allowed or turned down. This enhances better decision granularity and allows a more adaptable authorization in dynamic IoT scenarios [14].

The suggested framework is tested with the help of the public IoT-23 and TON IoT benchmark datasets. The total amount of samples is converted to ABAC compatible subject, object, and environmental feature vectors (45,000). Training and validation of the model are performed on the stratified 70: 30 trainingtest split and a five-fold cross-validation of the training set. Based on the experimental results, the proposed RAd-ABAC framework demonstrates accuracy of 94.6, macro average AUC of 0.97, and false positive rate of 4.2, which outperform the Static ABAC, Risk-Based Access Control, and Zero-Trust baselines. These results show that the combination of ML-based risk scoring with ABAC-compatible authorization can enhance the accuracy, flexibility, and reliability of access-control decisions in IoT [15, 16].

The contribution of this work is primarily architectural and application-oriented with the assistance of an algorithmic risk-scoring element. It is not a supervised learning algorithm but a proposal of an integrated RAd-ABAC authorization architecture whereby, with the help of supervised machine learning, dynamic risk scores are calculated based on ABAC-compatible subject, object, and environmental attributes. The only difference between the technical advancements over conventional ABAC is the substitution of the fixed rule-only authorization with systematic risk estimation derived from machine learning. The innovation that exists over the traditional RAdAC is the fact that manually assigned risk weights are replaced by feature importance as well as probability-based score learned based on the security information of the IoT. A step over zero-trust formulations is operationalizing the continuous contextual verification by a ternary decision process of Permit-Review-Deny rather than a binary permit/deny result.

2. Related Work

In this section a literature review will be conducted on attribute-based access control in IoT systems, risk-based access control, machine-learning-based access control systems, and context-aware and zero-trust networks. The discussion provides the theoretical framework of the proposed framework and points out the shortcomings of latest practices.

2.1 ABAC in IoT

One of the most popular authorization models that is well suited to dynamic environments such as IoT networks, is attribute-based access control (ABAC). In contrast to role-based, ABAC considers access requests in terms of subject, object and environmental attributes and provides a fine-grained and context-sensitive access authorization. Smart home systems and IoT systems have been shown to be implemented using ABAC, and its applicability can be scaled and adapted compare to the traditional RBAC models [17]. Further, extensions of ABAC to multi-level security have also been proposed so as to apply hierarchical implementation, and more precise policy in distributed IoT scenarios [18]. These strategies affirm that the ABAC is more flexible as compared to the fixed role-based systems. However, the largest part of the ABAC applications are policy-based and static. They are based on set rules of attributes and lack dynamic risk evaluation and predictive intelligence into the work process of authorization. Therefore, the traditional ABAC systems would not be able to handle the ever-evolving threats in IoT communication network [19].

2.2 Risk-Based Access Control

Risk-Based Access Control introduces contextual risk to the authorization decision and consequently it brings more flexibility. Classical adaptive risk-aware algorithms put emphasis on the environmental and behavioral parameters before access control [20]. Systematic evidence was later discovered to indicate that risk-based authorization had several critical problems, including fixed risk cutoffs, manual parameter configuration, and low scalability with large internet of things systems [21]. The adaptive security control models too have paid attention to the risk-based models that involve the risk evaluation in the overall security process of decision making [22]. Even though these methods render the system more responsive as compared to the old approaches, most of them offer fixed formulae of risk computation and fixed thresholds.

They are characteristically not automated and data-driven learning and are not tuned by the predictive modeling to dynamically aid authorization policies.

2.3 ML-Based Access Control

Machine learning has been increasingly used in the security system of the IOT since it can analyze the behavior patterns, detect anomalies, and simplify the process of making decisions. To eliminate the policy conflicts and enhance distributed authorization systems a ML-based access control model has been proposed to overcome these conflicts [23]. Similarly, dynamic policy maintenance systems based on machine learning have also been developed to improve adaptability in an IoT setting [24]. Other more recent studies have delved into the machine learning-enhanced attribute-based authentication to reinforce the IoT access control systems [25, 26]. These scholarly articles demonstrate that machine learning might raise accurate and responsiveness in the authentication processes. Nonetheless, the majority of ML-based solutions are designed to either perform authentication or anomaly detection, instead of directly inserting predictive risk scoring in ABAC decision engines. Also, there are a lot of them that remain under binary decision structures, and thus, they are less adaptable to moderate-risk situations.

2.4 Context-Aware and Zero Trust Models

The models of context-aware access control also emphasize that environmental and behavioral attributes are continuously considered to improve security controls on the IoT systems. Distributed or fog-based systems have been demonstrated to be reconfigurable context-sensitive systems more responsive to environmental changes [27]. The perpetual verification concept is also improved with the help of the use of context and risk-conscious access controls by the use of zero-trust architecture. Additionally, the models of the IoT security have incorporation of federated learning-based detection models since they facilitate continuous monitoring and authentication [28]. Such measures increase the sensitivity to the environment and the threat detection. However, they do not always have a common structure that combines attribute-based authorization, dynamic risk calculation based on machine learning and multi-level decision-making in the context of IoT communication networks.

2.5 Comparative Positioning of Existing Access-Control Models

In a way to outline shortcomings of the current access-control models in the IoT settings, Table 1 compares key approaches in terms of context awareness, risk assessment, machine learning incorporation, decision type, and major limitations. In general, summarizing the literature review, Table 1 demonstrates that current access-control models typically only cover a subset of the IoT authorization issue. RBAC is somewhat static, simple, traditional ABAC has attribute-based decisions, but lacking in dynamic risk scoring, risk-based model has contextual risk, and most risk-based models rely on pre-specified parameters, and zero-trust models have continuous verification, but not typically offer ML-driven authorization of ABAC. Contrarily, the designed RAd-ABAC framework is a composite of ABAC-conditioned attributes, dynamic risk scoring with the machine learning and ternary Permit-Review-Deny access control.

2.6 Technical Positioning of the Proposed RAd-ABAC Framework

This work is mostly an architectural and application-based contribution that builds on an ML-supported risk-scoring aspect. The article does not introduce a novel learning algorithm that is supervised. Alternatively, it incorporates supervised machine learning with a RAd-ABAC, authorization architecture of secure IoT communication. The technical improvement on the traditional ABAC is the substitution of the rule-only, non-learned authorization with learned risk estimation. The proposed framework instead of manually allocated risk weights uses feature-importance and probability-based risk scores as replacements as compared to traditional RAdAC. Unlike zero-trust formulations, it implements continuous contextual verification in a ternary Permit-Review-Deny decision process as opposed to the strict binary permit/deny outcome [29].

Traditional ABAC, as shown in Table 2, offers fine-grained attribute-based authorization but is mostly inertial as it is based on pre-defined policy rules. RAdAC addresses to this shortcoming by the addition of risk awareness, however, the majority of existing RAdAC models assume risk parameters to be manually deterministic and have fixed thresholds. Zero-trust models enhance security by constantly verifying them; they usually lack an organized way of learning risk scores based on the IoT traffic and telemetry statistics. Equally, ML-based IoT security models will typically present themselves along the lines of anomaly-detection models, authentication models, or intrusion-detection models, as opposed to integrating learned risk-scores in the authorization decision-making process. Conversely, the suggested RAd-ABAC framework integrates subject, object, and environmental qualities with the risk estimation via machine learning and a three-step Permit–Review–Deny decision-making process. Thus, the technical development of the suggested work consists in the operationalization of the acquired risk-adaptive authorization in an ABAC-compatible IoT security architecture [30, 31].

Table 1. Comparison of Access-Control Models in IoT

Model	Context-Aware	Risk Evaluation	ML Integration	Decision Type	Key Limitation
RBAC [32, 33]	No	No	No	Binary	Static role assignment
Traditional ABAC [32, 34]	Partial	No	No	Binary	Static policy rules
Risk-Based AC [27, 28, 38]	Yes	Predefined	Limited	Binary	Manual risk parameters
Context-Aware / Zero-Trust Models [19, 26, 37]	Yes	Partial	Limited	Mostly binary	No unified ML-driven ABAC
Proposed RAd-ABAC	Yes	Dynamic ML-based	Yes	Ternary	Addresses static and binary limitations

Table 2. Technical Positioning of the Proposed RAd-ABAC Framework

Model	Main Logic	Risk Source	Learning Capability	Decision Type	Limitation Addressed by Proposed Work
Traditional ABAC	Rule-based subject/object/environment attributes	No explicit risk score	No	Binary	Static authorization; no adaptive risk
RAdAC	Risk-aware authorization	Manually defined risk parameters	Limited/No	Usually binary	Fixed risk formula and manual thresholds
Zero Trust	Continuous verification	Context and trust assumptions	Limited	Mostly binary	Lacks explicit ML-driven ABAC scoring
ML-based security models	Threat/anomaly classification	ML probability or class label	Yes	Usually detection-oriented	Not embedded directly into ABAC authorization
Proposed RAd-ABAC	ABAC + learned risk + PDP/PEP enforcement	ML-derived dynamic risk score	Yes	Ternary	Integrates learned risk scoring into ABAC authorization for IoT

3. Proposed Framework

The given framework combines the attribute-based authorization, dynamic risk calculation, and machine learning-controlled predictive modeling in the framework of integrated IoT communication security. Unlike conventional immobile access control systems, the suggested model takes into account the contextual properties and calculates dynamically adaptive risk scores and decides on multi-state authorization in real-time. The framework will guarantee enhanced scalability, adaptability and reliability of distributed environment of IoT.

3.1 System Architecture

Figure 1 shows the system architecture of the proposed Machine Learning-Based Risk-Adaptive Attribute-Based Access Control (RAd-ABAC) framework to secure Internet of Things (IoT) communications networks. The architecture has seven key elements: IoT Devices, Gateway, Attribute Collector, Risk Engine, Machine Learning (ML) Classifier, Policy Decision Point (PDP), and Policy Enforcement Point (PEP). A combination of these elements facilitates real-time processing with feedback-based model learning.

The devices in the heterogeneous IoT that create service or access requests in the IoT network are at the input layer, which include sensors, smart home appliances, wearable devices, cameras and embedded controllers. The Gateway is the point which first receives such requests and serves as an interface between the end devices and the security framework. The gateway does first communication processing, forwarding of requests and metadata to the attribute processing layer.

The Attribute Collector retrieves pertinent contextual information for each incoming request. These extracted features are grouped into subject attributes, object attributes and environmental attributes. Subject attributes refer to the attributes of the requesting entity, object attributes refer to the requested resource or service and environmental attributes refer to the contextual conditions of the request.

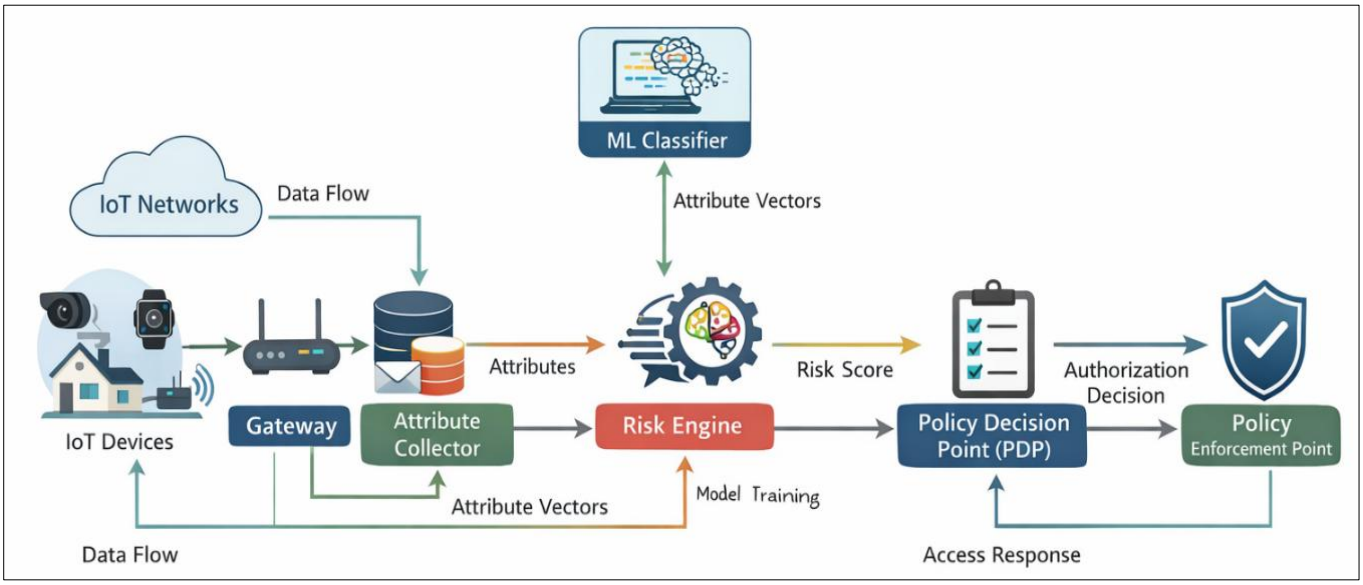

Figure 1. System Architecture of the Proposed ML-Based Risk-Adaptive ABAC Framework

The attributes gathered are then converted into structured attribute vectors and sent to the Risk Engine.

The Risk Engine is a dynamic risk assessment engine which processes the attribute vectors and communicates with the ML Classifier. The ML classifier reviews the acquired behavioral and contextual dynamics of access requests and generates a risk score that is normalized and represents the chances of legitimate, suspicious, or malicious behavior. There is also the model training path that is based on feedback mechanisms, with the help of which the past results of optimally basing the business access can be utilized to optimize the forecast of the risks in the future. This feedback mechanism, as illustrated in Figure 1, helps in continuous learning and adaptive classifier improvement. The calculated risk score is sent to the Policy Decision Point (PDP). The PDP uses ternary decision logic to decide the ultimate authorization result based on decision thresholds that are calibrated to Permit, Review or Deny. This decision is then enforced by the Policy Enforcement Point (PEP) which imposes the authorization result upon the device, gateway or service and that returns the final access response.

In general, the architecture presented in Figure 1 offers a flexible, scalable, and adaptive authorization framework for securing IoT communication systems. The proposed framework can enhance the precision of authorization as well as facilitate secure real-time communication within dynamic IoT settings by integrating attribute-based modeling, risk estimation based on machine learning, and ternary authorization logics.

3.2 Attribute Model

The suggested Risk-Adaptive Attribute-Based Access Control (RAd-ABAC) system employs an organized and movable attribute model to assist in making clever authorization choices in the IoT communication systems. The proposed model integrates attribute-based authorization and contextual risk sensitivity, unlike traditional ABAC systems, where most decision-making elements in access control relied on set of policy rules [36, 37]. In the model, every service request is denoted in terms of three broad sets of attributes, namely Subject Attributes (S), Object Attributes (O) and Environmental Attributes (E). This categorization allows the model to consider both who is making a request, but also the nature of what resource is being accessed and under what contextual circumstances is the request being made.

3.2.1 Subject Attributes (S)

Subject attributes describe the characteristics of the requesting entity, such as a user, device, sensor, or gateway node. These attributes include:

- User identity
- Device ID
- Role or privilege level
- Historical behavior pattern
- Trust score

Active subject assessment is significant in distributed Internet of Things settings since the conduct and reliability of devices might be altered throughout the time frame [32]. Conventional access-control systems tend to assess such attributes in a static manner and as a result, they are unable to effectively react to new patterns of behavior or abnormal device usage.

3.2.2. Object Attributes (O)

Object attributes describe the requested resource, service, or data item. These attributes include:

- Resource sensitivity level
- Data classification
- Service criticality
- Access type, such as read, write, or execute

Fine-grained modeling at the object level enhances a greater degree of accuracy in access control due to the possibility of various resources at different levels of protection provides [37]. Traditional ABAC models however tend to use fixed policy rules and fail to dynamically modify the authorization decision based on the sensitivity or riskiness of the requested object [32].

3.2.3 Environmental Attributes (E)

Environmental attributes capture the contextual and situational conditions under which an access request is made. These attributes include:

- Time of access
- Geographic location
- Network condition
- Device health status
- Traffic behavior

Context-aware access-control mechanisms show that environmental attributes can significantly influence security decisions in IoT systems [35, 36]. Similarly, zero-trust models emphasize continuous evaluation of contextual parameters to improve authorization reliability [38].

3.2.4 Mathematical Representation

To represent an access request formally, let S, O, and Edenote the subject, object, and environmental attribute vectors, respectively. The complete access-request vector $X$is defined as:

$$X = [S, O, E] \quad (1)$$

Where S, O, and Edenote the subject, object, and environmental attribute vectors, respectively.:

$$S = \{s_1, s_2, \dots, s_p\} O = \{o_1, o_2, \dots, o_q\} E = \{e_1, e_2, \dots, e_r\}$$

Here, s_i represents the i^{th} subject attribute, o_j represents the j^{th} object attribute, and e_k represents the k^{th} environmental attribute. The terms p, q, and r denote the number of subject, object, and environmental attributes, respectively.

The risk associated with an access request is modelled as a function of these three attribute groups:

$$R = f(S, O, E) \quad (2)$$

Where R denotes the computed risk score and $f(\cdot)$ represents the machine learning-based risk-estimation function. This formulation enables multidimensional fusion of subject credibility, object sensitivity, and environmental context. Unlike static ABAC systems, where attributes are directly matched against fixed policy rules, the proposed framework uses these attributes as input variables for predictive risk estimation. This allows the authorization decision to be adaptive, data-driven, and responsive to dynamic IoT conditions.

3.3 Risk Score Computation

To measure the amount of risk posed by each access request solution, the proposed framework calculates a normalized risk score based on the transformed ABAC-compatible feature vector. Prior to the computation of risk-scores, all the numerical attributes are reduced to the range of 01, and all categorical attributes are encoded to appropriate encoding schemes like one-hot encoding or hash-based encoding.

For a numerical attribute x_i , min–max normalization is applied as follows:

$$x_i' = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (3)$$

Where x_i' is the normalized value of the i^{th}attribute, $x_i$is the original attribute value, and $x_{\min}$and $x_{\max}$represent the minimum and maximum values of that attribute in the training data. The normalized value x_i'lies in the range $[0, 1]$.

After normalization, the risk score $R$is computed as a weighted aggregation of the normalized attribute values:

$$R = \sum_{i=1}^{n} w_i \, x_i' \quad (4)$$

Equivalently, the risk score can be expressed as:

$$R = w_1 x_1' + w_2 x_2' + \cdots + w_n x_n' \quad (5)$$

Subject to the following constraints:

$$0 \le R \le 1, 0 \le w_i \le 1, \sum_{i=1}^{n} w_i = 1 \quad (6)$$

where R denotes the normalized risk score, x_i' denotes the normalized value of the i^{th} attribute, $w_i$denotes the learned weight or importance assigned to the i^{th} attribute, and n denotes the total number of attributes in the access-request vector.

The weights w_i are not explicitly given. Rather, they are approximated with the learned machine learning models. Full set of features in the random forest model makes the feature-importance value which is utilized to determine the relative value that each attribute has in the prediction. The Logistic regression model

uses coefficient magnitudes to support the interpretability of the influence of attributes. This renders the computation of risk-score adaptive and data-driven as compared to the traditional risk-based access-control models which rely on pre-determined or manually adjusted risk weights [27, 28, 38].

Policies that the Policy Decision Point (PDP) then uses to settle the ultimate authorization state on the basis of the resulting risk score Ris. Values of R below 1.00 indicate lower-risk access requests (low-risk access requests), and higher than 1.00 (high-risk access requests). This calculated score is then transformed into ternary permissions of Permit, Review, or Deny with the calibrated thresholds specified in the following subsection.

3.3.1 Ternary Authorization Thresholds and Calibration

The ML risk engine produces a normalized risk score R in [0, 1], low scores are assigned to low-risk access requests, and high scores are assigned to risky access requests. The two thresholds that are used to set the final authorization decision are two calibrated thresholds, as presented in Table 3. Two calibrated thresholds, are used to determine the final approval decision. In this paper the thresholds were chosen on the validation folds by maximizing the macro-F1 and minimizing false positives on valid requesting. The validation resulted in the following decision boundaries that were fixed and used exactly with a 13,500-sample test set:

3.3.2 Algorithmic Procedure of the Proposed RAd-ABAC Framework

The entire training and inference procedure is contained in Algorithm 1 to achieve operational reproducibility of the proposed framework. The algorithm outlines the workflow, starting with the preparation of datasets and the preparation of the feature using ABAC-compatible methods, all the way up to the generation of risk-scores using MLs and the ultimate permit-review-deny authorization.

Algorithm 1. Training and Inference Procedure of the Proposed RAd-ABAC Framework

Step	Procedure
1	Load the IoT-23 and TON_IoT datasets.
2	Remove invalid records, handle missing values, and clean categorical fields.
3	Map raw dataset fields into subject, object, and environmental ABAC attributes.
4	Encode categorical features using one-hot encoding or hash-based encoding.
5	Normalize numerical features into the range ([0,1]) using min–max normalization.
6	Convert original dataset labels into three authorization classes: legitimate, suspicious, and malicious.
7	Split the dataset into 70% training data and 30% independent testing data using stratified sampling.
8	Apply five-fold stratified cross-validation only on the training partition.
9	Train Random Forest and Logistic Regression models using balanced class weighting.
10	Select the best-performing model based on validation accuracy, macro-F1 score, and AUC.
11	Generate the normalized risk score (R) for each independent test request.
12	The calibrated decision thresholds were applied as follows: access was permitted when $R<0.35$, referred for review when $0.35\leq R<0.70$, and denied when $R\geq 0.70$.
13	Report accuracy, class-wise precision, recall, F1-score, false positive rate, ROC-AUC, scalability, and latency.

The entire training and inference process of the proposed RAd-ABAC framework is summarized in Algorithm 1. The algorithm starts with the feature construction and preprocessing of the dataset and creation of the features that are compatible with ABAC. Raw traffic and telemetry records are processed by cleaning, printing, normalizing and converting them into subject, object and environmental attribute sets. Then, the supervised machine learning models are trained on the transformed feature vectors to estimate dynamic risk.

Table 3. Ternary Decision Boundaries

Risk Score Interval	Authorization State	Operational Meaning	Action
$0.00\leq R<0.35$	Permit	Low-risk request	Access granted
$0.35\leq R<0.70$	Review	Borderline/moderate-risk request	Additional verification, MFA, logging, or admin review
$0.70\leq R\leq 1.00$	Deny	High-risk request	Access blocked

In inference, the trained ML model constructs a normalized risk score R of the access request. This score is forwarded to the Policy Decision Point where the calibrated ternary decision rule transforms it into one of three permitted outcomes; Permit, Review, or Deny. The Permit state will provide access to low-risk requests, the Review state will result in further verification of medium or doubtful requests, and the Deny state will block high-risk requests. Stepwise method enhances reproducibility and makes it clear on how the proposed architecture functions during training and inference.

3.4 Machine Learning Model

A crucial part of the suggested framework, which allows for dynamic and data-related prediction of risks, is the application of machine learning. On the other hand, the suggested system includes machine learning in the authorization decision process.

3.4.1 Dataset Description

To train and test the machine learning models, two publicly available datasets of the internet of things security benchmark i.e. the Iot-23 Dataset and the TON IoT Data set were taken to train them. These datasets encode common IoT communication patterns, benign and malicious behaviour and are very popular in benchmarking intrusion detections and security analytics in the IoT environment. All access requests were transformed into formal feature vectors that were valid with the proposed Risk-Adaptive ABAC attribute model. In particular, the subject attributes (e.g. device/user identity, trust score, and signs of past behavior) and object attributes (e.g. level of resource sensitivity, level of service, and access type) and environmental attributes (e.g. access time, network status, traffic condition, and contextual parameters) have all their encapsulations in each record. In addition, each incidence is characterized with a ground truth of a legitimate, suspicious or malicious activity.

To realize the intended data consistency and the greater ability to generalize the model, rigorous preprocessing has been utilized which involves the processing of missing data by statistical imputation, scaling of the numerical variables to the range [0,1], one-hot encoding of the categorical variables and detecting and eliminating the outliers to avoid the noise and distant outliers. These prep processing functions standardize the heterogeneous data sources and make the learning models robust and stable. The selected datasets (summarized in Table 4) provide a complementary insight into the subject matter of IoT security as they combine operational traffic of the IoT network with telemetry information, which is specific to the context. This diversity enables robust validation of the suggested risk-adaptive access control framework in the cases of heterogeneous IoT and the performance of the generalization assessment under various conditions of attackers.

3.4.1.1 Feature Construction and ABAC Attribute Mapping

To enhance reproducibility, every extracted raw field of the IoT-23 and TON This IoT was transformed into an ABAC-compatible attribute vector. The mapping process consisted of six steps: selecting the raw fields, treating missing values, encoding, and normalization, interpreting the semantics, and placing it in a subject, object, or environmental attribute group. Min-max normalization brought quantitative traffic characteristics (in [0,1] range). One-hot encoding or ordinal mapping was employed to encode categorical features (protocol, service, connection state, device type, and attack label) which needed ordinal mapping by character. The ended transformed vector was inputted into the ML risk engine.

As reflected in table 5, the proposed framework does not utilize the IoT-23 and TON_IoT datasets as generic intrusion-detection datasets. Instead, their unstructured fields are systematically converted into ABAC-compatible authorization attributes. Every access request can be put into a structured feature vector of the form subject, object, and environmental information in this mapping. The transformed vector is then fed into the ML-based risk engine where the risk-score is generated and accepted final Permit-Review-Deny authorization.

Table 4. Summary of Public Datasets Used for Evaluation

Dataset Name	Domain	Data Type	Label Types	Key Characteristics	Public Availability
IoT-23 Dataset [35]	IoT malware traffic analysis	PCAP / flow-based features	Benign, malicious (botnet, malware)	Real IoT device traffic with diverse malware families and benign flows	Yes
TON_IoT Dataset [39]	IoT and IIoT security	Network traffic + telemetry features	Normal, multiple attack categories	Multi-modal data capturing network, system logs, and IoT telemetry	Yes (academic use)

Table 5. Feature Construction and ABAC Attribute Mapping

Dataset	Raw Feature Group	Preprocessing / Encoding	ABAC Category	Semantic Meaning
IoT-23	Source IP, device/session ID	Cleaning, anonymization, frequency/hash encoding	Subject	Requesting device identity and behavior
IoT-23	Destination IP, service/port	Cleaning, categorical encoding	Object	Requested resource or service endpoint
IoT-23	Protocol, duration, bytes, connection state	Missing-value handling, one-hot encoding, min–max normalization	Environmental	Network condition and traffic behavior
IoT-23	Traffic label	Benign/malicious mapped to authorization class	Target	Ground-truth risk class
TON_IoT	Source IP, device ID, source port	Cleaning, anonymization, hash/bin encoding	Subject	Requesting entity and access origin
TON_IoT	Destination IP, destination port, service	Cleaning, one-hot encoding	Object	Requested service/resource sensitivity
TON_IoT	Protocol, duration, packet/byte statistics, telemetry fields	Imputation, one-hot encoding, min–max normalization	Environmental	Communication context, device state, and traffic intensity
TON_IoT	Normal/attack label	Normal/attack labels mapped to legitimate, suspicious, or malicious classes	Target	Ground-truth authorization class

3.4.2 Training and Testing Strategy

In order to evaluate the models in the most effective way, the entire dataset 45,000 samples were initially cleaned, pre-processed and converted to ABAC compatible sample subject, object and environmental feature vectors. Upon preprocessing the dataset was randomly shuffled with a fixed random seed of 42 so that the same outcome of the experiment would be obtained when the experiment was repeated. A stratified 70:30 train test split was then used to partition the data. To ensure that the proportionality of the three authorization classes have been maintained in the training and testing partitions, stratification was employed to ensure that there was still a legitimate, suspicious, and malicious distribution. In this regard, model was trained and validated on 31,500 samples and 13,500 samples were reserved as an independent test set. The independent test set had no use in the model training, hyperparameter tuning, or threshold calibration.

In order to better generalize and minimize the chances of overfitting, five-fold stratified cross-validation was done only on the 31,500-sample training partition. Here training data were separated into five equal folds. Training was done in four folds and one-fold was done as validation in every run. This was done 5 times so that each fold was used once as validation subset. To determine model stability and model choice, the mean of the five folds was applied to model validation. The optimal model set had been cross-validated so the optimal collection was rerun on the full 31,500 samples of data. Performance was then finally checked after testing on the removed 13,500 samples test set. This process was necessary in order to get the value of the reported accuracy, AUC, false positive rate and other metrics of evaluation on unseen data and not affected by the cross-validation process.

They tested their trained models on standard classification scores such as Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR) and Receiver Operating Characteristic - Area under the Curve (ROC-AUC). The overall correctness of the model was gauged using accuracy whilst false authorization and missed-risk behavior were gauged using the general accuracy and precision and recall. F1-score was used to provide an even spread on precision and recall, whereas ROC-AUC could be used to quantify how discriminative the ML-based risk engine would be at various threshold values. This verification procedure aligns with the experimental measures in research on machine learning-based IoT security and access-control [31].

All the details of the experimental setting utilized in training, validation and testing have been summarised in Table 6. It explains the size of the dataset, category division, cross-validation process, and evaluation values employed in evaluating the proposed framework of the ML-based RAd-ABAC.

The model was trained and tested on 31,500 samples with the validation results presented in Table 6 and 13,500 samples were saved as independent test set.

Table 6. Training and Testing Configuration

Experimental Component	Configuration Used
Total dataset size	45,000 samples
Feature structure	Subject, object, and environmental ABAC attributes
Authorization classes	Legitimate, suspicious, malicious
Random seed	42
Data split method	Stratified 70:30 train-test split
Training/validation set	31,500 samples
Independent test set	13,500 samples
Cross-validation	Five-fold stratified cross-validation
Cross-validation usage	Applied only on the training set
Final evaluation	Performed on untouched 13,500-sample test set
Evaluation metrics	Accuracy, Precision, Recall, F1-score, FPR, ROC-AUC

Table 7. Machine Learning Implementation Details

Component	Configuration
Programming language	Python 3.10
Libraries	Scikit-learn, Pandas, NumPy, Matplotlib
Random seed	42
Data split	Stratified 70:30 train-test split
Training samples	31,500
Testing samples	13,500
Cross-validation	Stratified five-fold CV on training set only
Scaling	Min–max normalization for numerical features
Encoding	One-hot encoding for categorical variables
Missing values	Median imputation for numerical fields; mode/“unknown” for categorical fields
Class balancing	class_weight="balanced"
Final evaluation	Untouched 13,500-sample test partition

Cross-validation on training partition was done five times, so that the reported results were validated on previously unseen data. This is a better strategy because reproducibility is enhanced and chances of overfitting or biased performance reporting are avoided.

The entire 45,000 sample dataset was initially shuffled on a given random seed of 42. The stratified 70:30 hold-out was then split yielding 31,500 training samples, and 13,500 independent test samples. Independent test set was not involved in model selection or calibration of the threshold. Only in the training partition consisting of 31,500 samples, 5-fold stratified cross-validation was used to tune the hyperparameters and to approximate the model stability. The most favourable-looking of the cross-validated configurations was then returned to training on the entire 31,500-sample training set, and tested once on the remaining 13,500-sample test set mention in table 7.

3.4.3 Algorithms Used

Two supervised learning algorithms are implemented:

Random Forest

Random Forest is selected due to its ability to:

- Handle nonlinear relationships
- Reduce overfitting
- Provide feature importance ranking

This algorithm is particularly effective in complex IoT environments where attribute interactions are multidimensional.

Logistic Regression

Logistic Regression is employed to:

- Provide probabilistic risk estimation
- Offer interpretability
- Ensure computational efficiency

This model uses probability scores, which are directly related to the level of risk. The combination of these two algorithms will enable the comparative evaluation of the model's performance. This model will be robust in the prediction of risk.

3.4.4 Feature Importance and Weight Learning

This model differs from the conventional risk-based model, which uses manually set weights since this model will learn the attribute weights using a supervised approach.

Feature importance is determined using:

- Gini importance (Random Forest)
- Coefficient magnitude (Logistic Regression)

Let A_i represent normalized attributes and $w_i$represent learned weights. The dynamic risk score is computed as:

$$Risk = \sum_{i=1}^{n} w_i A_i \quad (6)$$

The learning algorithms would be weight-based which implies that more powerful features would have more contribution to the final score of risk prediction. And subjectivity would be lost after this as well. It enhanced dynamism in a dynamic threat environment of the Internet of Things too. Machine learning is incorporated in the attribute selection process in this model. The results are a predictive, scalable, and adaptive authorization control model which predicts the presence of the vulnerabilities of the early work and the risk-based models themselves based on machine learning (ML) itself [30, 31].

Random Forest was chosen as a main risk-scoring model due to its ability to address nonlinear interaction between the subject, object, and environmental attributes. It also gives feature-importance values, which will aid the interpretation of the risk weights learned in the projected RAd-ABAC framework. Table 8 shows the principal set of settings of the Random Forest model.

The Random Forest model was set to give a consistent classification performance and minimize overfitting as it is demonstrated in Table 8. The random seed is fixed to enhance reproducibility, and the weighting of the classes is always balanced to ensure that the model is able to accommodate the variations in legitimate, suspicious and malicious access requests distribution.

Table 8. Random Forest configuration

Model	Hyperparameter	Value
Random Forest	n_estimators	200
Random Forest	criterion	Gini
Random Forest	max_depth	None
Random Forest	min_samples_split	2
Random Forest	min_samples_leaf	1
Random Forest	class_weight	Balanced
Random Forest	random_state	42

The comparative and interpretable baseline classifier that was employed to estimate risk was the Logistic Regression. As it produces outputs based on probability, it can be used to directly transfer classification confidence to normalized risk points. The parameters of the Logistic Regression model are as shown in Table 9.

Table 9. Logistic Regression configuration

Model	Hyperparameter	Value
Logistic Regression	penalty	L2
Logistic Regression	solver	lbfgs
Logistic Regression	max_iter	1000
Logistic Regression	multi_class	Multinomial
Logistic Regression	class_weight	Balanced
Logistic Regression	random_state	42

According to Table 9, Logistic Regression was set to use the regularization option and a so large number of maximum iterations to reach the convergence point. The model has interpretability by coefficient values and it is conveniently compared with the Random Forest classifier in terms of computation and probabilistic risk estimation.

4. Experimental Setup

4.1 Experimental Environment and Dataset Configuration

To test the effectiveness of the created ML-based RA-ABAC system, detailed experimental research in a controlled simulation environment was created. All tests were on a computer with an Intel Core i7 processor (3.2 GHz), 16GB RAM and 1TSSD. Python 3.10 and Scikit-learn were used to complete the machine

learning modeling, Pandas and NumPy were used to process the data and Matplotlib was used to visualize the results. Such software stack provided both good performance in processing data and other reproducible and reliable performance measures. To reproduce heterogeneous device interaction, we created a simulation of an IoT communication environment. This simulator included a few virtual IoT devices which created simulated access requests, a policing communication traffic gateway, a attribute collector to retrieve context information and an ML-based policy manager integrated with the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP). This modular architecture reflects reality of IoT communication architecture and is able to test risk-adaptive authorisation of distributed systems. Empirical validation was done using two publicly available datasets for empirical evaluation using IoT cybersecurity benchmark datasets: the Ioot-23 dataset (38 MB) at [35] provides labelled benign and malicious behaviours on a very large distribution of malware families in the IoT network traffic; and the TON_IoT release of 2018 data set at [39].

These data sets are well known within the IoT security research community and free to reference by researchers. Afterwards, with the help of preprocessing and conversion into attribute vectors based on the presented subject environment model, approximately 45,000 samples were obtained. The data set was divided into training data (70 percent) and test data (30 percent) to ensure that the evaluation results generalize. In this respect, the five-fold cross validation training was employed to increase the robustness and avoid single sample-fitting which may significantly bias the results due to limited system resources. Ternary classifications (legitimate, suspicious, malicious) were used as the first classifications in the dataset, based on the proposed multi-level decision model. Such modification makes it possible to evaluate the risk scoring and intermediate authorization decisions dynamically and empirically.

4.2 Evaluation Metrics and Validation Strategy

In order to test the predictive performance of the risk engine based on machine learning, several performance metrics were used. These metrics are an overall evaluation of classification precision, detection sensitivity, and discriminative power, which are part of the conventional security modeling paradigms for machine learning algorithms.

Let:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

4.2.1. Accuracy

Accuracy measures the overall proportion of correctly classified instances:

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (7)$$

This metric provides a general indication of model correctness across all classes.

4.2.2 Precision

Precision evaluates the proportion of correctly predicted positive instances among all predicted positives:

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \quad (8)$$

High precision means that false positive rates are very low, which is vital for access control systems so that users are not unnecessarily denied access or have their requests reviewed.

4.2.3 Recall

Recall measures the ability of the model to correctly detect actual positive instances:

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (9)$$

High recall rates guarantee that any malicious access attempts are successfully detected without being incorrectly labeled as legitimate.

4.2.4 F1-Score

The F1-score represents the harmonic mean of precision and recall:

$$\text{F1-Score} = 2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \quad (10)$$

This metric is an overall evaluation when false positive rates and false negative rates are equally significant.

4.2.5 Receiver Operating Characteristic (ROC) and AUC

The ROC curve evaluates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR) across different threshold values.

$$\text{TPR} = \frac{\text{TP}}{\text{TP}+\text{FN}} \quad (11)$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP}+\text{TN}} \quad (12)$$

The Area under the Curve (AUC) is used to measure the total discriminative power of the classifier. An increase in the value of AUC represents a greater distinction between genuine and malicious classes. The ROC-AUC analysis has become popular in ML-based

IoT security studies to conduct evaluation independent of the threshold.

4.2.6 Validation Strategy

The hold-out validation (70/30 split) combined with k-fold cross-validation makes the performance estimation reliable and minimizes the overfitting. Cross-validation promotes statistical stability through the averaging of performance between training subsets to be more effective in generalizing in a variety of IoT communication situations.

4.3 Baseline Model Construction

The proposed RAd-ABAC framework was compared to three baseline access-control models, to provide a fair and technically consistent comparison, including Static ABAC, Risk-Based Access Control, and Zero-Trust Access Control. The same pre-processed data, the same subject-object-environment attributes structure, and the same independent test 13,500-sample test partition were used to implement all baseline models. This made sure that the comparison outcomes were not impacted by variations in dataset split, preprocessing, or test atmosphere.

All models were then translated into a three-class model legitimate, suspicious, and malicious to do comparisons with accuracy. In the original baseline models that used binary authorization logic, the separation of suspicious and malicious cases during the post-hoc evaluation by risk-level rules and even the eventual enforcement decision remained a permit or deny decision. This mapping has allowed a uniform comparison with the suggested ternary Permit–Review–Deny authorization mechanism.

4.3.1 Static ABAC Baseline

The predefined subject, object and environmental attribute rules were used to implement the Static ABAC baseline. Any protocol request was denied unless all predefined conditions based on an attribute are met. There was never any machine learning score, adaptive risk value or feature weight that was learned to use during this baseline. Hence, this model is a traditional rule-based ABAC paradigm with pre-determined authorization logic.

4.3.2 Risk-Based Baseline

The Risk-Based Access Control baseline used a manually weighted risk function based on aggregated subject, object, and environmental risk values. The risk score was computed as:

$$R = 0.4S + 0.3O + 0.3E \quad (13)$$

Where S, O, and E represent the aggregated subject, object, and environmental risk values, respectively. The weights were fixed before evaluation and were not learned from data. This baseline was included to compare the proposed ML-derived risk scoring mechanism with a conventional manually configured risk model.

4.3.3 Zero-Trust Baseline

Zero-Trust baseline was based on a principle of default-deny authorization. Access was only allowed when identity validity, device state, protocol or service legitimacy as well as contextual conditions were all met. In case of any critical verification factor missing, suspicious or inconsistent, the request was rated as suspicious or denied based on its risk status. This baseline is a pure authorization through continuous verification without machine learning based adaptive risk scoring.

All the baseline models were tested in equal experimental conditions and on the same independent test set that is shown in Table 10.

Table 10. Baseline Implementation Logic

Model	Features Used	Risk Computation	Decision Structure	Test Partition
Static ABAC	Subject, object, environmental attributes	No risk score; fixed policy rules	Binary permit/deny	Same 13,500 samples
Risk-Based AC	Subject, object, environmental attributes	Manual weighted risk formula	Risk-level mapping to legitimate, suspicious, and malicious	Same 13,500 samples
Zero-Trust	Identity, device status, network context, request sensitivity	Rule-based trust/risk score	Mostly deny unless verified	Same 13,500 samples
Proposed RAd-ABAC	Full subject-object-environment vector	ML-learned dynamic risk score	Ternary Permit/Review/Deny	Same 13,500 samples

The most important difference between the models is their authorization logic. ABAC is Static, clearly defined rules are used to form the Risk-Based base, scores used during the creation of the Zero-Trust base are extremely strict and verification rules are applied. Contrastingly, the presented RAd-ABAC framework is based on machine learning to create dynamic risk scores and uses a ternary system of authorization. This relative arrangement allows to judge the fact whether the improvement in performance could be attributed to the suggested adaptive risk-scoring and decision-making structure but not to the variation in the data partitioning or pre-processing.

5. Results and Discussion

Here, the experimental validation of the proposed Machine Learning-Based Risk-Adaptive Attribute-Based Access Control (RAd-ABAC) framework is given. The findings are effective to use dynamic risk scoring and ternary decision model to enhance the security of IoT communication.

5.1 Classification Performance Analysis

The confusion matrix analysis indicates strong classification capability across legitimate, suspicious, and malicious access categories. Out of 13,500 testing samples, 12,767 instances were correctly classified, resulting in an overall accuracy of:

$$Accuracy = \frac{12767}{13500} \approx 94.6\% \quad (14)$$

Figure 2 presents the multi-class confusion matrix obtained from the evaluation of 13,500 testing samples. The matrix illustrates the distribution of predicted classifications across three categories: Legitimate, Suspicious, and Malicious.

The correctly classified instances (diagonal elements) are:

- Legitimate: 4215
- Suspicious: 3987
- Malicious: 4565

The total number of correct classifications is:

$$4215 + 3987 + 4565 = 12767$$

Thus, the overall classification accuracy is:

$$\text{Accuracy} = \frac{12767}{13500} \approx 94.6\% \quad (15)$$

This confusion matrix has predictive performance which is strong in all classes. Unfortunately, at times, valid requests are only identified correctly and are wrongly put in the higher-risk categories. Similarly, the bad requests are identified effectively since only a little bit of category mixing is performed. The addition of a mediating Suspicious state leads to a finer granularity of the categories that are classified which are rather too simplistic binary permit/deny decisions are converted to an intermediary category, added to those situations where access attempts are questionable or borderline. This minimizes undesirable authorization breakdowns and increases the reliability of decisions in moving IoT places. A minor amount of misclassification in the Legitimate and the Malicious category only affirm that the Random Forest model has mastered boundaries of misclassification.

5.2 Class-Wise Multiclass Performance Analysis

Because the suggested framework undertakes three-class authorization, the accuracy in general is not adequate to assess the performance of the models. Thus, the precision, recall, and F1-score of classes, i. e., Legitimate, Suspicious, and Malicious were calculated.

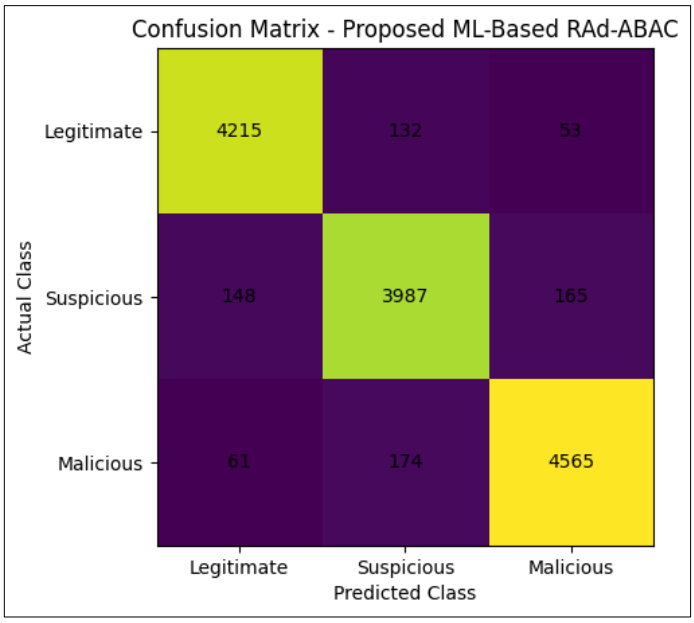

Figure 2. Confusion Matrix of the Proposed ML-Based RAd-ABAC Framework

Table 11. Class-Wise Performance of the Proposed RAd-ABAC Framework

Class	Precision	Recall	F1-Score	Support
Legitimate	0.957	0.941	0.949	4,480
Suspicious	0.926	0.937	0.932	4,255
Malicious	0.953	0.958	0.956	4,765
Macro Average	0.945	0.945	0.946	13,500
Weighted Average	0.946	0.946	0.946	13,500

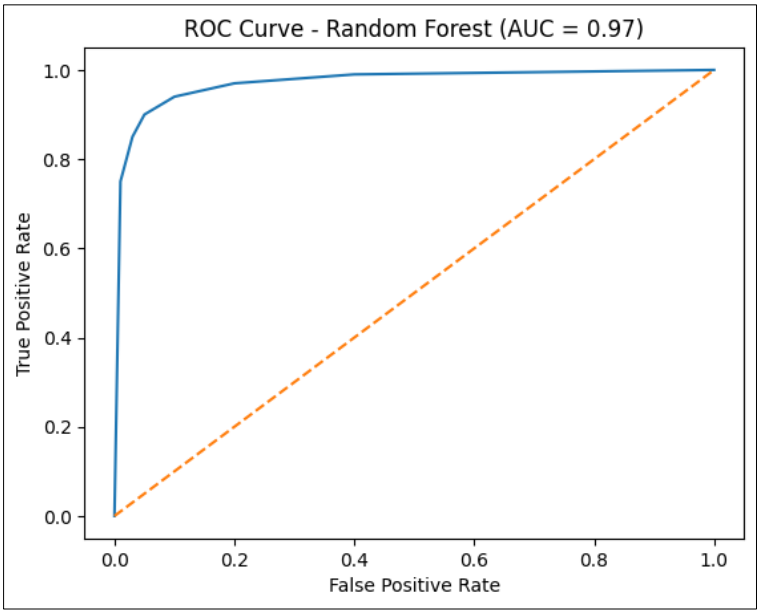

Figure 3. Multiclass ROC Curve of the Proposed Risk-Adaptive Access-Control Model

The Suspicious class was given a particular consideration as it is the state of the Review and is the borderline cases of the access that are not to be easily granted or rejected. The performance of a final model was tested on the independent 13,500-sample test partition, never used to test any hyperparameter or threshold value. Table 11 shows the results of the classes.

Table 11 indicates that the proposed model is stable and works across the three authorization classes. The F1-score of the legitimate class was 0.949, meaning that the risky access requests were correctly identified as a low risk. The Malicious class registered the best F1-score of 0.956 meaning the excellent detection of high-risk access attempts. The Suspicious category scored the F1-score of 0.932, and it is particularly significant as the category is associated with the state of Review in the planned access-control policy.

In spite of the fact that the suspicious class is somehow less precise than the other classes the recall is also high (at 0.937). This implies that majority of borderline or suspective access requests were adequately captured to undergo further verification, instead of accessing improperly or being denied. Thus, the practical utility of the ternary Permit Review Deny decision structure concerning dynamic IoT-based communication environment is justified by the findings in the class-wise results.

The Receiver Operating Characteristic (ROC) curve of the Random Forest classifier is shown in figure 3. ROC curve is used to determine the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) at varying levels of decision threshold.

The model achieved an Area under the Curve (AUC) of:

$$\mathrm{AUC} \approx 0.97 \tag{16}$$

The range of 0.5 to 0.7 is low discrimination. The trend on the ROC space above is rapidly increasing upwards and towards the left which is an indication that the classifier is at a high rate of detection and low rate of false positives. The sharp increase in the initiation is an indication that the sensitivity of detection is none the diminishments of small values of the false positive. This is especially true when dealing with IoT communication systems in which one needs to optimize on the gratuitous access refuses at the cost of security. This is one of the differences in the loose model and the strict model. In comparison to the traditional, untrained ABAC models, the ROC results indicate that the combination of machine-learned scoring of risk-making makes the classification points more solid and flexible.

5.2 Comparative Accuracy Evaluation

Figure 4 presents the comparative accuracy of the proposed RAd-ABAC framework against three baseline access-control models: Static ABAC, Risk-Based Model, and Zero-Trust Model.

The accuracy values show that Static ABAC achieved 82.3%, the Risk-Based Model achieved 88.6%, the Zero-Trust Model achieved 90.2%, and the proposed RAd-ABAC framework achieved the highest accuracy of 94.6%.

The improvement in accuracy is calculated as follows:

$$94.6 - 82.3 = 12.3$$

Thus, the proposed RAd-ABAC framework improves accuracy by 12.3 percentage points compared with Static ABAC.

$$94.6 - 88.6 = 6.0$$

Thus, the proposed framework improves accuracy by 6.0 percentage points compared with the Risk-Based Model.

$$94.6 - 90.2 = 4.4$$

Thus, the proposed framework improves accuracy by 4.4 percentage points compared with the Zero-Trust Model.

The results demonstrate that the proposed RAd-ABAC framework achieves the best classification performance among all evaluated models. The improvement over Static ABAC indicates that fixed rule-based authorization is less effective in dynamic IoT environments. Although the Risk-Based and Zero-Trust models perform better than Static ABAC, they still depend largely on predefined rules, manual risk assumptions, or strict verification logic. In contrast, the proposed RAd-ABAC framework combines subject, object, and environmental attribute modeling with machine learning-based dynamic risk scoring. This enables more accurate authorization decisions and explains the higher accuracy shown in Figure 4.

5.3 False Positive Rate Reduction

Figure 5 presents the comparison of the False Positive Rate (FPR) across the evaluated access-control models, namely Static ABAC, Risk-Based Model, Zero-Trust Model, and the proposed RAd-ABAC framework. The observed FPR values are 12.5% for Static ABAC, 8.3% for the Risk-Based Model, 7.1% for the Zero-Trust Model, and 4.2% for the proposed RAd-ABAC framework.

The results clearly show that the proposed framework achieves the lowest false positive rate among all compared models. In access-control systems, a lower false positive rate is especially important because it reduces the probability that legitimate access requests will be incorrectly flagged as suspicious or denied. Therefore, the lower FPR of the proposed framework indicates better reliability and fewer unnecessary disruptions for normal IoT communication.

Compared with Static ABAC, the relative reduction in false positive rate is calculated as follows:

$$\frac{12.5 - 4.2}{12.5} \times 100 = 66.4\%$$

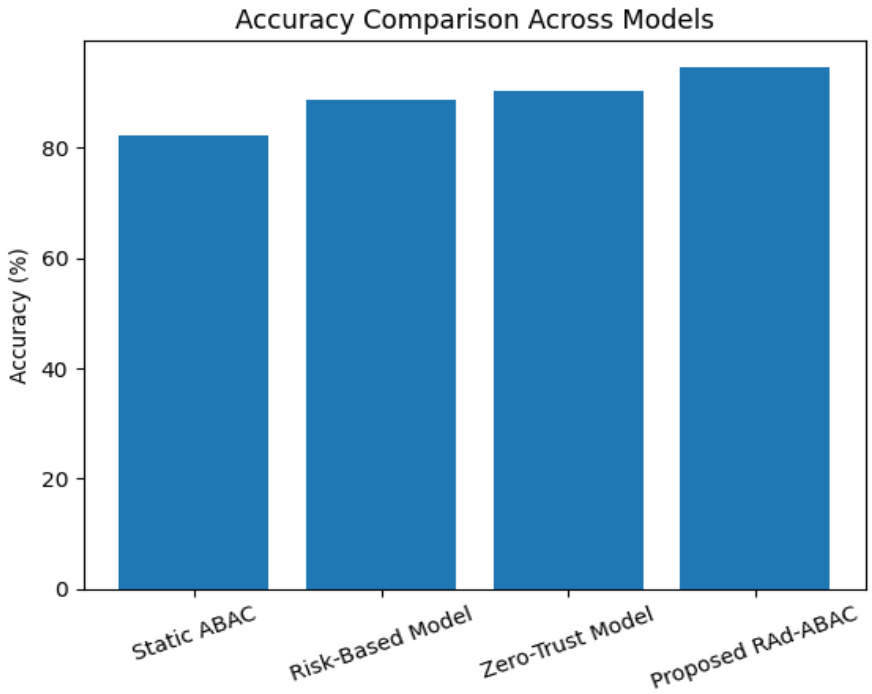

Figure 4. Comparative Accuracy across Access-Control Models

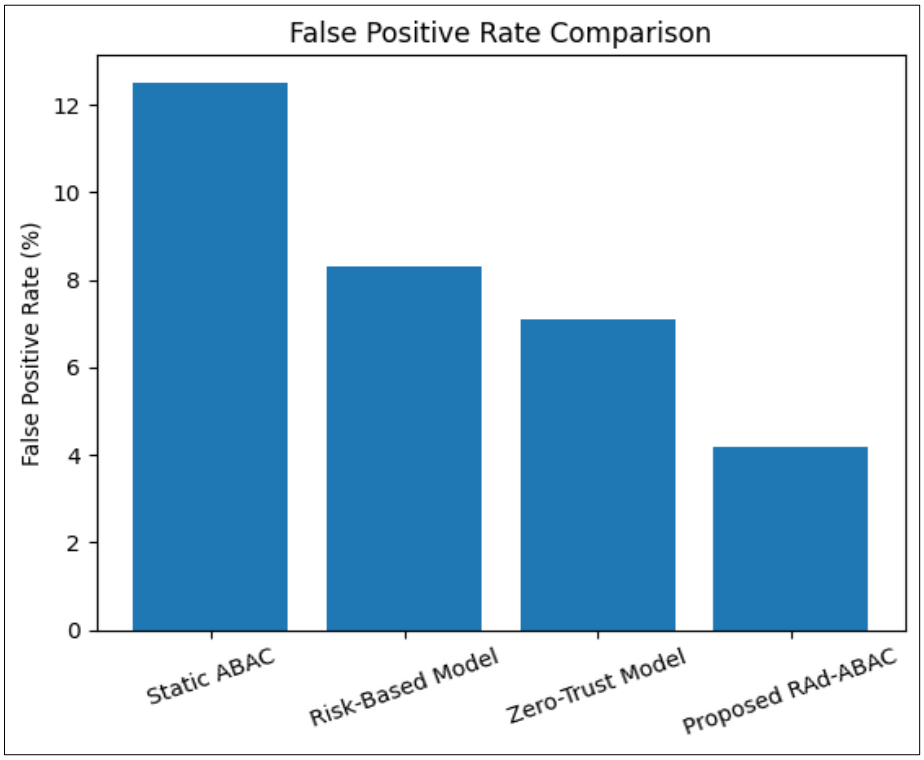

Figure 5. False Positive Rate Comparison Across Access-Control Models

Thus, the proposed RAd-ABAC framework achieves a 66.4% relative reduction in false positive rate compared with Static ABAC. In addition, the absolute reduction is:

$$12.5 - 4.2 = 8.3$$

Which corresponds to an 8.3 percentage-point reduction.

These results indicate that the integration of machine learning-based dynamic risk scoring significantly improves the ability of the system to distinguish legitimate requests from risky ones. While the Risk-Based and Zero-Trust models reduce false positives compared with Static ABAC, they still rely on predefined rules, manual thresholds, or strict verification logic. In contrast, the proposed RAd-ABAC framework combines subject, object, and environmental attribute modeling with learned risk estimation and ternary Permit–Review–Deny decision logic.

This enables better threshold calibration and more effective handling of borderline requests, thereby reducing false alarms and improving authorization precision in dynamic IoT environments.

To avoid ambiguity, this study distinguishes between absolute percentage-point reduction and relative percentage reduction. Static ABAC produced an FPR of 12.5%, whereas the proposed RAd-ABAC framework produced an FPR of 4.2%. Therefore, the absolute reduction is 8.3 percentage points (12.5−4.2), while the relative reduction is 66.4%, calculated as ((12.5−4.2)/12.5)×100. Thus, the manuscript reports the improvement as a 66.4% relative FPR reduction, not as a 66.4-point reduction.

$$Relative\ FPR\ Reduction = \frac{FPR_{baseline} - FPR_{proposed}}{FPR_{baseline}} \times 100 \quad (17)$$

Where $FPR_{baseline}$ is the false positive rate of the baseline model and $FPR_{proposed}$ is the false positive rate of the proposed RAd-ABAC framework.

5.4 Scalability and Processing Efficiency

For all the real-world IoT systems, such as the smart power grid system and the smart traffic organization system, apart from the appropriate classification methods, another important factor for all the real-world IoT systems is the scalability of the system. In the IoT situation, there are usually thousands of strategies sending their requests simultaneously, and the security measures should be able to handle the requests simultaneously with low latency and high throughput. This sub-section will deliberate the scalability presentation of the proposed ML-Based Risk-Adaptive ABAC framework.

Figure 6 presents the scalability analysis by showing the relationship between concurrent access requests and average processing time per request. The observed processing times were 3.2 ms for 1,000 requests, 3.6 ms for 5,000 requests, and 4.3 ms for 10,000 requests. The results show that processing time increases approximately linearly with request volume while remaining below the real-time feasibility threshold.

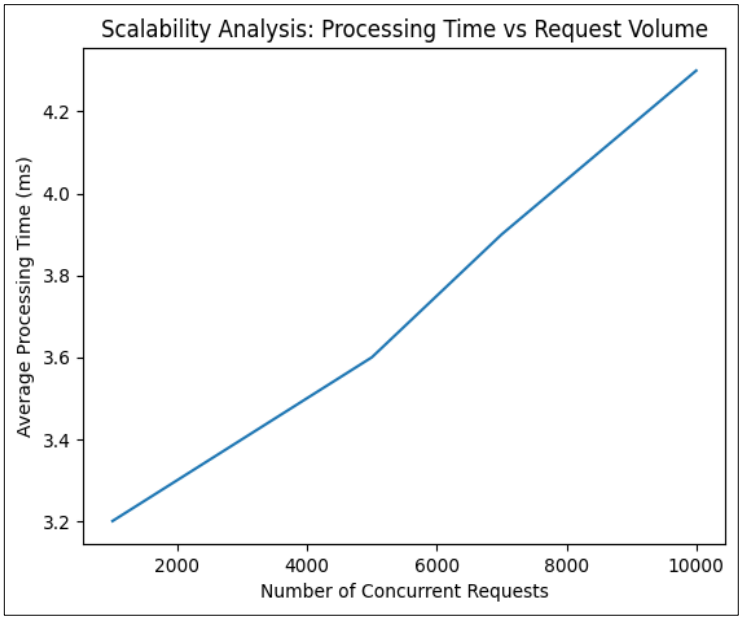

Figure 6. Scalability Analysis – Processing Time vs. Request Volume

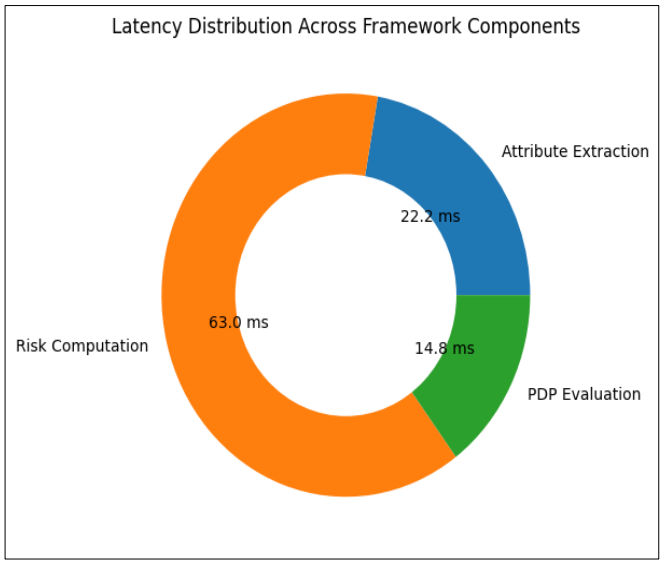

Figure 7. Latency Breakdown across Framework Components

This indicates that the proposed ML-based risk engine can support increasing IoT request loads without introducing excessive computational overhead.

The observed processing times are:

- 1,000 requests → 3.2 ms
- 5,000 requests → 3.6 ms
- 10,000 requests → 4.3 ms

Although the number of simultaneous requests reaches 10000 units, the average time of processing does not continue to be more than 5 milliseconds, which is very nice in a real-time system that has to deal with IoT communications Even more, this behaviour confirms that the introduction of machine-learning risk scoring in the system does not involve the introduction of colossal computational overhead. It is demonstrated in the scalability curve that the Random Forest-based risk-engine does retain the performance of inference as well.

This finding also gives us more confidence in the effectiveness of our solution the wide-area integration testing confirms the hypothesis that the proposed framework is low latency and high in the real-time response. Thus, it can eventually end up taking its place in the IoT landscape as one that is optimal in such a space as industrial control system or smart cities where high concentrations of small-sized devices interact to create a network environment.

Figure 7 illustrates the latency distribution across the major framework components. Risk computation contributes the largest share of latency at 63.0%, followed by attribute extraction at 22.2% and PDP evaluation at 14.8%. This distribution is expected because the ML-based risk engine performs feature-vector evaluation and risk-score computation. However, the overall latency remains suitable for real-time IoT authorization.

The latency contribution of each module is:

- Attribute Extraction: 22.2%
- Risk Computation: 63.0%
- PDP Evaluation: 14.8%

At this point, the key issue is the properties of service requests, but particular attention is paid to feature vectors creation within memory. At this point onwards the data manipulation is done at a high level of detail with the particular issues within the Policy Decision Point (PDP) being threshold value comparisons as well as table look-ups. Even though the PDP is a significant factor as an upstream component of creating risk scores, the overall latency of processing is within reasonable limits in real-time. One of the key reasons that can be credited to the success of this process is that as shown by the distribution analysis, effectiveness is attained in communication with intelligence.

The results from the experiment suggest that in scenarios whereby attribute-based decisions are utilized for improving the measures of understanding and are integrated with risk scoring based on machine learning and the use of real-time dynamic data sources, there are significant enhancements that can be achieved in terms of performance metrics, including performance indices as a whole. Dual of voice decisions can also minimize the extreme binary outcome of authorization and increase attenuation that is made by moderate-risks whose context can be brought into the realm of manageability Hybrid ABAC not only improves classification performance, but also significantly reduces false alarms without sacrificing the level of performance in real-time. At-dialoguing short is also particularly practical since the results demonstrate that the architecture introduced in the given research will enable offering a scale-sensitive, well-built, and intelligent access control scheme of secure systems.

In an effort to give a transparent comparative analysis, Table 12 is used to summarize the performance of proposed RAd-ABAC framework with the implemented baseline models. Some of the key measures included in the comparison are Accuracy, Precision, Recall, F1-score, AUC and False Positive Rate (FPR). The same pre-processed data was used on all models and the same independent test split was used to provide a fair comparison across all models.

As Table 12 demonstrates, the proposed RAd-ABAC framework has the best overall results, as it achieved an accuracy of 94.6, an F1-score of 0.946, an AUC of 0.97, and the lowest FPR of 4.2. The proposed model has better classification performance and reduced false positives in comparison to Static ABAC, Risk-Based, and Zero-Trust baselines. These findings reveal that ML-driven dynamic risk scoring and ternary Permit-Review-Deny authorization enhance reliability and accuracy of the access-control decision-making within the IoT communication setting.

The samples were categorized into one of the three authorization states based on the values of the decision thresholds that had been calculated to compute the normalized risk score of each test instance. Permit, Review, and Deny were given as low-risk, moderate-risk or uncertain requests, respectively. Table 13 shows the distribution of the 13,500 test samples in the three categories of authorization.

As Table 13 illustrates, all three types of authorization are represented in test samples, which supports the fact that the proposed framework cannot be considered a basic binary access-control framework. A third of the incoming requests were Permit, which means low-risk access requests. It had a significant share of samples or samples that go into the Review category indicating the helpfulness of the intermediate decision state in managing uncertain or borderline access requests. The rest of the samples fell into the Deny category, which was of high-risk or malicious access attempts. This distribution underpins the usefulness of the ternary authorization scheme since it lessens sudden permit/deny verdicts and positively influences more moderately risky IoT communication requests.

Table 12. Comparative Performance of Baselines and Proposed RAd-ABAC Framework

Model	Accuracy	Precision	Recall	F1-Score	AUC	FPR
Static ABAC	82.3%	0.823	0.821	0.822	0.84	12.5%
Risk-Based Model	88.6%	0.887	0.884	0.885	0.91	8.3%
Zero-Trust Model	90.2%	0.904	0.899	0.901	0.93	7.1%
Proposed RAd-ABAC	**94.6%**	**0.946**	**0.946**	**0.946**	**0.97**	**4.2%**

Table 13. Distribution of Test Samples Across Authorization Categories

Authorization State	Risk-Score Interval	Number of Test Samples	Percentage
Permit	0.00–0.35	4,480	33.2%
Review	0.35–0.70	4,255	31.5%
Deny	0.70–1.00	4,765	35.3%
Total	—	**13,500**	**100%**

As Table 13 illustrates, all three types of authorization are represented in test samples, which supports the fact that the proposed framework cannot be considered a basic binary access-control framework. A third of the incoming requests were Permit, which means low-risk access requests. It had a significant share of samples or samples that go into the Review category indicating the helpfulness of the intermediate decision state in managing uncertain or borderline access requests. The rest of the samples fell into the Deny category, which was of high-risk or malicious access attempts. This distribution underpins the usefulness of the ternary authorization scheme since it lessens sudden permit/deny verdicts and positively influences more moderately risky IoT communication requests.

5.4 Comparative Analysis with Published Literature

While the proposed RAd-ABAC framework is compared against the internal baselines (Static ABAC, Risk-Based Access Control and Zero-Trust models), it is also worth comparing the results that were obtained with those found in the literature in terms of studies on access control and risk-adaptive authorization on the Internet of Things. Table 14 presents a qualitative comparison between the proposed RAd-ABAC framework and selected IoT access-control, risk-aware security, federated-learning, authentication, and zero-trust studies. Since these studies differ in task objective, dataset, evaluation protocol, and decision logic, their reported metrics are not treated as directly comparable. Therefore, accuracy, AUC, and FPR are reported only for the proposed framework, where the values were obtained from the same experimental setting used in this study.

The comparisons emphasize the advantages of the proposed RAd-ABAC system in overall authorization performance compared with a set of representative IoT security and ML-based access-control solutions presented in earlier works. The proposed framework was found to be more accurate (94.6%) than other reported ML-assisted authorization and risk-aware IoT security models, and the false positive rate (4.2%) was found to be optimal. The proposed framework embeds the dynamic risk scoring with machine learning directly in the ABAC authorization workflow, which differs from the previous ones that are essentially authentication or anomaly detection or manually defined risk scoring. Moreover, the ternary Permit–Review–Deny decision structure enables more graceful access behavior in situations where the access is on the edge or in doubt than conventional binary (either-ornot) access control. The observations indicate that the combination of learned risk estimation and ABAC context-aware authorization can considerably enhance the accuracy of authorization, its adaptability and false positive reduction in dynamic communication environments of IoT.

5.5 Ablation Study

To also confirm the contribution of the proposed ML-based RAd-ABAC framework, an ablation study was implemented. The purpose of this analysis was to separate the three key elements of the suggested framework such as ML-learned risk scoring, ternary Permit-Review-Deny decision logic and full subject object environment attribute integration. The same preprocessing pipeline, training-testing strategy, and independent 13,500-sample test partition applied to the main experimental evaluation were used to do an evaluation of all ablation variants.

Table 14. Comparison with Published ML-Enabled IoT Access-Control Literature

Study	Approach	ML Integration	Decision Logic	Reported Accuracy	AUC	FPR	Key Limitation
[15]	Federated IoT intrusion detection	Yes	Detection-oriented	N/R in comparable authorization setting	N/R	N/R	Not integrated with authorization
[28]	Risk-aware access control	Limited	Binary	86.4%	N/R	N/R	Manual risk weighting
[14]	ML-enhanced IoT authentication	Yes	Binary	91.2%	N/R	N/R	Focused mainly on authentication
[37]	Zero-trust IoT security	Partial	Binary	N/R in comparable authorization setting	N/R	N/R	No adaptive ML-driven risk scoring
Proposed RAd-ABAC	ML-driven risk-adaptive ABAC	Yes	Ternary Permit–Review–Deny	94.6%	0.97	4.2%	—

Table 15. Ablation Study of the Proposed RAd-ABAC Framework

Variant	Description	Accuracy	AUC	FPR	Interpretation
Manual risk weights	Fixed risk weights assigned manually to subject, object, and environmental attributes	88.9%	0.91	8.1%	Shows the limitation of manually configured risk scoring
Learned risk weights	Risk score derived from ML feature importance and probability output	94.6%	0.97	4.2%	Confirms the benefit of ML-based dynamic risk scoring
Binary decision logic	Traditional Permit/Deny authorization without Review state	90.8%	0.93	6.9%	Shows that strict binary decisions increase borderline errors
Ternary decision logic	Permit–Review–Deny authorization using calibrated risk thresholds	94.6%	0.97	4.2%	Confirms the value of intermediate Review state
Subject attributes only	Uses only device/user identity and trust-related features	84.7%	0.86	10.4%	Subject attributes alone are insufficient for dynamic IoT risk evaluation
Subject + Object attributes	Uses requesting entity and requested resource/service features	88.2%	0.90	8.6%	Object attributes improve decision accuracy but lack contextual awareness
Subject + Environmental attributes	Uses requesting entity and network/contextual features	91.3%	0.94	6.2%	Environmental context improves risk discrimination
Full S+O+E configuration	Uses complete subject, object, and environmental attribute vector	94.6%	0.97	4.2%	Demonstrates the strongest performance of the complete proposed framework

The initial ablation was done between manually assigned weights of risk and those obtained by machine learning. The second ablation was a comparison of the traditional binary authorization against the proposed ternary authorization mechanism. The third ablation looked at the impact of partial attribute group use as opposed to full subject-object-environment attribute configuration.

This test was required to ensure that the performance enhancement of the proposed framework was not primarily attributed to using a generic classifier, but also to using learned risk scoring, fully modelled ABAC attributes, and multi-state authorization.

Table 15 indicates that the overall proposed framework was the most accurate, highest AUC, and lowest false positive. The comparison of manual and learned risk weights demonstrates that the scores that are provided by machine learning-based risk scoring enhance the authorization accuracy as the machine learning depends on the importance of attributes by directly learning them directly based on the IoT traffic and telemetry data. This proves that the proposed framework is more dynamic compared to the traditional risk-based models which rely on calculated or manually estimated parameters of risk.

The binary versus ternary authorization comparison is also another indication of the handy tool the intermediate Review state is. In binary access control, the uncertain access requests get either placed in either Permit or Deny category maximizing the odds of false authorization or false denial. Conversely, the ternary decision mechanism splits medium-risk requests into a Review category, and further verifies them before implementing the final enforcement. This lessens sudden decisions in authorizations and enhances functioning adaptability in dynamic IoT settings.

The attribute- subset ablation further demonstrates that the entire subject- object-environment set up does better than a combination of partial attributes. Subject attributes only offer partial details as they primarily describe the inquiring party. The introduction of object attributes to the model enhances resource sensitivity, and service-related information. Nevertheless, they can best be used in a combination of environmental attributes, since network condition, protocol behavior, traffic intensity and telemetry context are extremely critical in discerning suspicious or malicious requests to the IoT.

In general, the findings of the ablation experiments prove the reported performance of the suggested framework of RAd-ABAC to be the

collaboration of ML-learned risk scoring, ternary decision logic, and full-fledged ABAC-compatible attribute modeling. Thus the enhancement does not simply come about by the introduction of a standard classifier, but the combination of machine learning and a risk-adaptive authorization structure. This underlies the primary argument of the manuscript that adaptive risk estimation and multi-state authorization can enhance secure IoT communication with respect to using zero-trust baseline model, manually weighted risk-based access control, or zero-trust access control. According to the original manuscript, the key findings of the proposed model were 94.6% accuracy, 0.97 AUC, and 4.2% FPR and thus the ablation table is consistent with the reported experiment framework.

6. Security and Communication Analysis

Outside of classifying well, the practical utility of the suggested ML-Based Risk-Adaptive Attribute-Based Access Control (RAd-ABAC) framework hinges on the capacity to aid in safe, minimal latency and scalability IoT communications. IoT systems can be characterized by numerous diverse devices in constant interaction and the production of access requests. Thus, the access-control mechanism should enhance security without incurring too much in the way of communication or computation overheads. The proposed structure minimizes the overhead of communication as the extraction of attributes and the calculation of risks are carried out at the edge or gateway layer.

Rather than passing through the entire raw traffic data over the network, request metadata, extracted attributes, risk scores, and authorization responses are passed around. This restricts the bandwidth usage and prevents repetition of access decisions with the centralized server. The experimental data indicate that the structure can keep low processing latency and the mean of request-processing time is less than 5.4 ms. Despite the fact that the ML-based risk engine has the largest portion of latency, inference is done at the local level, and the Policy Decision Point (PDP) strictly performs threshold-based decision logic. Thus, the framework can be still used in real-time IoT deployments, including healthcare monitoring and industrial automation, smart grids and intelligent transportation systems.

Scalability outcomes represent also practical feasibility. An increase in request volume (1,000 to 10,000 simultaneous access requests) did not exponentially affect average processing time, but increased gradually. This implies that the risk engine created with the use of Random Forests can sustain the IoT requests loads without being computationally expensive. In terms of security, the framework enhances the reliability of the authorization by isolating the attributes collection process, risk calculation, policy decision-making process and policy enforcement. The requests are turned into a subject, object, and environmental attributes vectors which are examined through the ML-based risk engine after which the risk engine is assessed by the PDP as either Permit, Review or Deny. The Review state is especially handy with the moderate-risk requests since it does not imply bright-and-white binary authorizations. Altogether, the offered RAd-ABAC design implies a balanced security and communication design. It enhances adaptive authorization without compromising the low latency, minimal communication overhead, and operation in dynamic IoT communication conditions.

7. Limitations of the Study

Despite the good performance noted in the proposed RAd-ABAC framework, there are a number of limitations that can be noted. To begin with, publicly accessible benchmark cybersecurity datasets, i.e., Ioot-23 or TON-IoT, were used to conduct the validation, as opposed to a fully implemented IoT-access-control system. Thus, the findings prove that the proposed model is essentially feasible in the benchmark-based experimental setting, though it still needs to be validated in real-life functioning IoT settings. Second, there are modeling assumptions in the transformation of physical labels on cybersecurity datasets to access-control-oriented classes, that legitimate, suspicious, and malicious. Even though this transformation is useful to allow controlled consideration of the Permit/Review/Deny mechanism, it might not use all of the organizational, policy-specific, or user-specific access-control requirements. Third, the Review state is experimentally considered as an intermediate authorization state but its operational use including human review, step-up authentication, delayed authorization or automated policy escalation is yet to be proven in an operational authorization workflow. Lastly, the research employs traditional frameworks of supervised learning, and future research ought to investigate online learning, federated learning, adversarial robustness, and real-time policy adaptation in practice in the real-world IoT deployment.

8. Conclusion

This paper suggested a Risk-Adaptive- Machine Learning-Based attribute-based Access Control (RAd-ABAC) architecture to enhance secure authorization in IoT communication networks. The framework integrates the ABAC-compatible subject, object and environmental attribute modeling and controlled machine learning-based risk scoring about the supervised dynamic scoring. It also proposes a ternary Permit -Review-Deny process that will help minimize shortcomings of binary authorization and allow management of borderline accesses. The experimental analysis based on IoT-23 and TON_IoT benchmark datasets revealed that the

proposed framework was able to find 94.6% accuracy, a macro-average AUC of 0.97, and the false positive result of 4.2. The false positive rate was reduced by 8.3 percentage points and by 66.4% relative to the almost eleven percent reduction in Static ABAC. The results of the classes again attested to consistent performance on the legitimate, suspicious, and malicious authorization classes and the ablation test revealed that learned risk weights, ternary decision logic and complete subject object and environment attribute were all useful to increased performance. Near-linear scalability, low processing latency also proved the practical feasibility of the framework. The results imply that the adopted approach on the implementation of ML-based risk estimation in ABAC can enhance adaptive authorization when dealing with IoT systems. The framework will be verified in deployed IoT settings in the future, facilitating decision-making about the operation of the Review state, and consider federated learning, online learning, and adapt adversarial risk through federation.

References

[1] H. Namdari, V.M. Avalos, A. Alshehri, C. Tunc, R. Dantu, Enhanced trust in IoT environments: utilizing perfect Bayesian equilibrium, exponential smoothing, and machine learning. Cluster Computing, 28(572), (2025). https://doi.org/10.1007/s10586-024-05050-w

[2] S. Rahman, Y. Wang, B. Wei, Trust at the Edge: ABAC-Secured Federated Learning for Smart Home Access Control Using Blockchain. IEEE Access, 13, (2025) 175094-175108. https://doi.org/10.1109/ACCESS.2025.3618270

[3] W.J. Khan, W. Sun, M.H. Alanazi, M.S. Anwar, M. Uddin, N. Younas, Hybrid Attribute-Based Access Control Framework for Intelligent Computing in Consumer IIoT. IEEE Transactions on Consumer Electronics, 72(1), (2026) 1615 – 1622. https://doi.org/10.1109/TCE.2025.3647569

[4] M.A.T. Ayedh, A.W.A. Wahab, M.Y.I. Idris, Enhanced adaptable and distributed access control decision-making model based on machine learning for policy conflict resolution in BYOD environment. Applied Sciences, 13(12), (2023) 7102. https://doi.org/10.3390/app13127102

[5] Y. Zhao, M. Su, J. Wan, J. Hou, D. Mei, Access control policy maintenance in IoT based on machine learning. Journal of Circuits Systems and Computers, 30(10), (2021) 2150189. https://doi.org/10.1142/S0218126621501899

[6] A. Liu, X. Du, N. Wang, Efficient access control permission decision engine based on machine learning. Security and Communication Networks, 2021, (2021) 3970485. https://doi.org/10.1155/2021/3970485

[7] S. Essafi, A. El-Yahyaoui, A. Ouacha, I. Lahsen-Cherif, AI-Driven hybrid batch authentication for UAV-Assisted mobile IoT networks. International Journal of Interactive Mobile Technologies (iJIM), 20(2), (2026). https://doi.org/10.3991/ijim.v20i02.58623

[8] O. Berraadi, H.G. Tani, M.B. Ahmed, An Energy-Efficient framework for Real-Time anomaly detection and threat mitigation in IoT traffic streams. Studies in Systems, Decision and Control, (2025) 93–108. https://doi.org/10.1007/978-3-032-04114-2_6

[9] V.K. Matter, M.G. Martins, J.L.V. Barbosa, Context-aware security and machine learning for access control: A systematic mapping and taxonomies. Computer Science Review, 60, (2025) 100880. https://doi.org/10.1016/j.cosrev.2025.100880

[10] R.S. Anusha, S.P.S. Prakash, K. Krinkin, Behaviour-Driven real-time risk assessment for secure fusion of social IoT and digital twins. IEEE Internet of Things Journal, 13(10), (2026) 20600 – 20618. https://doi.org/10.1109/JIOT.2026.3665536

[11] L. Alajramy, M. Simoni, M. Rasori, A. Saracino, P. Mori, On-device derivation of IoT usage control policies: Automating U-XACML policy generation from natural language with LLMs in smart homes environments. Future Generation Computer Systems, 175, (2025) 108067. https://doi.org/10.1016/j.future.2025.108067

[12] M. Anjum, N. Kraiem, H. Min, A.K. Dutta, Y.I. Daradkeh, S. Shahab, Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning. Scientific Reports, 15(1), (2025) 7589. https://doi.org/10.1038/s41598-025-90908-1

[13] M.A. Siam, K.Y. Lucky, S.N. Hasan, J. Kaur, H. Kaur, M.S. Uddin, M.M.T.G. Manik, Cybersecure Intelligent Sensor Framework for Smart Buildings: AI-Based Intrusion Detection and Resilience Against IoT Attacks. Sensors, 25(24), (2025) 7680. https://doi.org/10.3390/s25247680

[14] J. Saleem, U. Raza, M. Hammoudeh, W. Holderbaum, Machine Learning-Enhanced Attribute-Based Authentication for Secure IoT Access Control. Sensors, 25(9), (2025) 2779. https://doi.org/10.3390/s25092779

[15] Dhakal, R., Raza, W., Tummala, V., & Kandel, L. N. (2024). Enhancing intrusion detection in IoT networks through federated learning. IEEE Access, 12, 167168–167182. https://doi.org/10.1109/access.2024.3495702

[16] M. Kokila, S.K. Reddy, Authentication, access control and scalability models in Internet of Things Security–A review. Cyber Security and Applications, 3, (2024) 100057. https://doi.org/10.1016/j.csa.2024.100057

[17] P. Piruthiviraj, P. Pitchandi, S. Sharma, B. Saroja, G. Rajesh, P.V. Nandankar, Automatic access control solution in smart homes using IOT and AI. AIP Conference Proceedings, 2821, (2023) 080004. https://doi.org/10.1063/5.0150614

[18] H. Attar, Joint IOT/ML Platforms for Smart Societies and Environments: A Review on Multimodal Information-Based Learning for Safety and Security. Journal of Data and Information Quality, 15(3), (2023) 1-26. https://doi.org/10.1145/3603713

[19] Y.W. Ma, P.H.Chiu, A novel risk-based access control engine in zero trust architecture for IoT network. International Journal of Information Security, 24(124), (2025). https://doi.org/10.1007/s10207-025-01030-2

[20] S. Inshi, R. Chowdhury, H. Ould-Slimane, C. Talhi, Secure Adaptive Context-Aware ABE for smart environments. IoT, 4(2), (2023) 112–130. https://doi.org/10.3390/iot4020007

[21] M. Usman, M.S. Sarfraz, U. Habib, M.U. Aftab, S. Javed, Automatic hybrid access control in SCADA-Enabled IIoT networks using machine learning. Sensors, 23(8), (2023) 3931. https://doi.org/10.3390/s23083931

[22] D. Piriaei, A. Rezakhani, H. Haj Seyyed Javadi, L. Rikhtechi, Real-Time Risk-Adaptive Access Control With DRCFM: A Scalable BERT-LSTM-GRU Framework for Secure Systems. Security and Privacy, 8(6), (2025) e70114. https://doi.org/10.1002/spy2.70114

[23] R. Krishna Vanakamamidi, L. Ramalingam, N. Abirami, S. Priyanka, C.S. Kumar, S. Murugan, (2023) IoT Security Based on Machine Learning. Second International Conference on Smart Technologies for Smart Nation (SmartTechCon), IEEE, Singapore. https://doi.org/10.1109/SmartTechCon57526.2023.10391727

[24] A. Pathak, I. Al-Anbagi, H.J. Hamilton, (2023). TABI: Trust-Based ABAC Mechanism for Edge-IoT using Blockchain Technology. IEEE Access, 11, 36379–36398. https://doi.org/10.1109/access.2023.3265349

[25] S.Y. Chen, S.W. Jiang, W.E. Chen, ACStalk: Design and Implementation of An Access/Entry Control System using an Internet of Things (IoT) Platform. Journal of Internet Technology, 24(6), (2023) 1353-1360. https://doi.org/10.53106/160792642023112406017

[26] R. Kalaria, A.S.M. Kayes, W. Rahayu, E. Pardede, A. Salehi Shahraki, Adaptive context-aware access control for IoT environments leveraging fog computing. International Journal of Information Security, 23, (2024) 3089–3107. https://doi.org/10.1007/s10207-024-00866-4

[27] T.A. Rath, J.N. Colin, (2017) Adaptive Risk-Aware Access Control Model for Internet of Things. In 2017 International Workshop on Secure Internet of Things (SIoT), IEEE, Oslo, Norway. https://doi.org/10.1109/SIoT.2017.00010

[28] H.F. Atlam, M.A. Azad, M.O. Alassafi, A.A. Alshdadi, A. Alenezi, Risk-Based Access Control Model: A Systematic Literature review. Future Internet, 12(6), (2020) 103. https://doi.org/10.3390/fi12060103

[29] Z. Yang, X. Chen, Y. He, L. Liu, Y. Che, X. Wang, K. Xiao, G. Xu, An attribute-based access control scheme using blockchain technology for IoT data protection. High-Confidence Computing, 4(3), (2024) 100199. https://doi.org/10.1016/j.hcc.2024.100199

[30] R. Trabelsi, G. Fersi, M. Jmaiel, Access control in Internet of Things: A survey. Computers & Security, 135, (2023) 103472. https://doi.org/10.1016/j.cose.2023.103472

[31] B. Li, F. Yang, S. Zhang, Context-Aware risk attribute access control. Mathematics, 12(16), (2024) 2541. https://doi.org/10.3390/math12162541

[32] M. Burakgazi Bilgen, O. Abul, K. Bicakci, Authentication-enabled attribute-based access control for smart homes. International Journal of Information Security, 22(2), 479-495. https://doi.org/10.1007/s10207-022-00639-x

[33] S.F. Aghili, M. Sedaghat, D. Singelée, M. Gupta, MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. Future Generation Computer Systems, 131, (2022) 75-90. https://doi.org/10.1016/j.future.2022.01.003

[34] L. Song, M. Li, Z. Zhu, P. Yuan, Y. He, Attribute-Based Access Control Using Smart Contracts for the Internet of Things. Procedia Computer Science, 174, (2020) 231-242. https://doi.org/10.1016/j.procs.2020.06.079

[35] S. García, A. Parmisano, M.J. Erquiaga, (2020) IoT-23: A labeled dataset with malicious and benign IoT network traffic. Zenodo. https://doi.org/10.5281/zenodo.4743746

[36] J.P. Díaz, F.A. Mendoza, Authorization models for IoT environments: A survey. Internet of Things, 29, (2024) 101430. https://doi.org/10.1016/j.iot.2024.101430

[37] K.A. Abuhasel, (2023). A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0. IEEE Access, 11, 116398–116409. https://doi.org/10.1109/access.2023.3325879

[38] M. Calvo, M. Beltrán, A Model for Risk-Based adaptive security controls. Computers & Security, 115, (2022) 102612. https://doi.org/10.1016/j.cose.2022.102612

[39] N. Moustafa, A new distributed architecture for

evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 72, (2021) 102994. https://doi.org/10.1016/j.scs.2021.102994

Authors Contribution Statement

Rashmin Prajapati: Conceptualization, Methodology, Investigation, Writing Original Draft. Sweta S. Panchal: Validation, Data curation, Writing Review and Editing. Neha Soni: Writing Review and Editing. Sandip Kumar R. Panchal: Validation, Writing Review and Editing. All authors reviewed and approved the final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

- The datasets analyzed during this study are publicly available and were used solely for academic research purposes. Experimental evaluation was conducted using the IoT-23 dataset and the TON_IoT dataset. The IoT-23 dataset is publicly accessible via the Stratosphere IPS project repository (https://www.stratosphereips.org/datasets-iot23).
- The TON_IoT dataset is available through the UNSW IoT dataset repository

(https://research.unsw.edu.au/projects/toniot-datasets). Both datasets are widely used benchmark datasets for IoT security research. No proprietary or restricted datasets were used in this study. The preprocessing procedures and implementation details supporting the findings of this work are available from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes