Machine Learning in BYOD Security: Three-Layered Access Control Framework for Enhanced Threat Detection and Policy Management

Aljuaid Turkea Ayedh M ^{1,2*}, *Ainuddin Wahid Abdul Wahab* ^{1,3}, *Mohd Yamani Idna Idris* ^{1,4}

[1]Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, Malaysia.
[2]Faculty of Computer Science and Information Technology, Shaqra University, Shaqra, Saudi Arabia.
[3] Center of Research for Cyber Security and Network, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia.
[4] School Center for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia.
Email: taljuaid@su.edu.sa

ABSTRACT

Existing access control provides a security solution to manage BYOD policies but is limited to controlling and providing adequate security. This paper comprehensively implements access control encompassing three security layers of the BYOD policy simultaneously: tactical, strategic, and operational. This system comprises the initial component and dynamic attributes for enforced access decisions. The second component consists of risk monitoring and anomaly detection algorithms. Finally, the third component employs the adaptive policy adjustment algorithm, which provides recommendations to the administration for policy updates in cases of abnormal access based on the results of the attack detection algorithm. The suggested access control solution was implemented using machine learning algorithms to detect anomalous and atypical user behavior. The experimental results obtained from the UNSW-NB15 dataset confirmed that the proposed access control could improve the anomaly detection algorithm and adaptive policy adjustment performance while reducing prediction detection time. The results demonstrated that the risk monitoring and anomaly detection algorithm, with a prediction time of 0.5 seconds and an accuracy rate of 0.95 percent, is the most effective method for monitoring attacks. Additionally, the results indicated that the accuracy of the adaptive policy adjustment algorithm was approximately 97%, with a threshold value of 0.26 being the optimal modification threshold value. The solution could enhance the detection of insider threats, access control, and policy management while at the same time making access control dynamic, adaptable, flexible, and secure.

Keywords: Access Control; BYOD Security; Machine Learning; Risk Monitoring; Anomaly Detection Algorithms; Policy Monitoring and Administration; Three Security Layers.

1.0. INTRODUCTION

The Bring Your Own Device (BYOD) model signifies a notable advancement in the consumerization of Information Technology (IT), allowing workers to use their devices inside a corporate framework [1]. This concept provides several advantages, including financial savings for businesses and improved employee productivity. Nonetheless, it also presents significant security and privacy problems. The ubiquity of cybersecurity concerns, such as illegal access, possible corporate data breaches, violations of user confidentiality, and the emergence of harmful actions inside the digital corporate landscape, highlights these issues [2]. Therefore, comprehensive access control solutions are needed to address these challenges and security vulnerabilities in complex and dynamic environments.

Prior research has suggested methods for access control; however, these primarily concentrate on a unique layer of secure control policies and lack a holistic approach appropriate for BYOD policies. Researchers including Kim et al. [3] and Lee et al. [4] have introduced an access control model intricately integrated inside the tactical layer based on an authentication policy governing the interaction between BYOD devices and an organization's network resources. Nonetheless, its shortcomings are apparent since it needs to integrate real-time risk controls that analyze the dynamic behavioral characteristics of access requests. Thus, the inherently static characteristics of these models limit their flexibility in many circumstances.

Subsequent research has suggested access control predicated on the strategic layer, emphasizing risk policy and attack detection. Yin et al. [5] presented a risk-based access control system and an MLP-based intrusion detection system employing a unique hybrid feature selection technique, IGRF-RFE, using filter and wrapper feature selection strategies, MLP multi-classification accuracy increases from 82.25% to 84.24%. Hyojoon et al. [6] created an Intrusion Detection Hyperparameter Control System (IDHCS) employing PPO-based reinforcement learning to control a deep neural network (DNN) feature extractor and k-means clustering module. The method attained an accuracy of 94.268%. Bhardwaj et al. [7] devised an innovative risk access control model that integrates a stacking sparse AutoEncoder (AE) with a Deep Neural Network (DNN) for network traffic classification, attaining an accuracy of 82.4% while employing a support vector machine algorithm that achieved 75.5% accuracy.

Despite these advancements, previous solutions may remain ineffective in a BYOD environment due to their limited scope and failure to provide the required security across several layers. A complete review of various access control performance metrics, such as attack detection accuracy, prediction time, and adaptive policy modification accuracy, is required to increase the resilience of present approaches. Therefore, access control in the intricate and evolving BYOD environment must concurrently address three tiers of security policies: operational (adaptive policy management), tactical (dynamic authentication policy based on risk factors), and strategic (real-time risk monitoring and anomaly detection) to attain balanced access control and threat detection with flexibility and adaptability.

Therefore, this paper suggests access control via machine learning techniques encompassing three BYOD policy levels: operational, tactical, and strategic. The suggested methodology has three essential components: dynamic risk assessment decision-making, real-time risk monitoring using anomaly detection to identify unusual user behaviors and an adaptive policy adjustment algorithm that suggests policy modifications in response to irregular access patterns. This comprehensive strategy employs machine learning methods to identify and react to unusual user actions by modifying access controls, accordingly, presenting considerable promise for improving the identification of insider security concerns. The model handles dynamic and complicated circumstances by integrating real-time risk measures in the decision-making framework and securely responds to unexpected access requests. This study improves insider threat assessment, access control, and policy administration to provide a dynamic, adaptable, and flexible BYOD-specific access control system.

The proposed access control system strategic methodologies are distribution based, density-based, statistical, and neural network-based algorithms. These methodologies enhance access decision-making by identifying anomalies and assessing real-time risks. This model's efficacy was assessed using the UNSW-NB15 dataset, demonstrating that dynamic, granular authorization policies, combined with the Random Forest anomaly detection algorithm and adaptive policy modification, yield a resilient access control solution. Experimental findings demonstrate a detection accuracy 95% with a reaction time of around 0.5 seconds. Additionally, anomaly detection and adaptive policy modifications have a 97% accuracy rate. This work's primary contributions may be encapsulated as follows:

- Assess the shortcomings of existing access control solutions and provide a holistic strategy that integrates all three tiers of an optimal security policy: operational, tactical, and strategic. This methodology must encompass secrecy, integrity, and parameters for attack detection.
- Examine particular concerns inside each tier of security policies. The operational layer has to focus on addressing policy management and administrative issues. The tactical layer needs to enhance adaptability, while the strategic layer should focus on performance optimization, especially in real time situations.
- Improve both the effectiveness of access control and the detection of insider threats by integrating real-time access control methods with improved attack detection techniques.
- Utilize four strategic methodologies: distribution-based algorithms, density-based algorithms, statistical-based algorithms, and neural network-based algorithms to implement risk monitoring and anomaly detection algorithms. These methods improve access decision-making by utilizing real-time risk monitoring and anomaly detection.
- Introduce an adaptive adjustment algorithm that automates the recommendation of access policy enhancements, contingent upon the policy administrator's approval.
- Perform an analysis of real-time risk monitoring and anomaly detection algorithms utilizing the UNSW-NB15 dataset. Perform experiments before and after data processing to assess the accuracy of attack detection and the time required for prediction compared to other algorithms.
- Contrast the proposed access control system's performance with benchmarks that have been established in prior studies that have employed the same dataset for evaluation.
- Optimize policy management, enhance the detection of insider threats, and improve access control to establish a dynamic, adaptable, and flexible access control system.

This work is structured as it follows: The subsequent section, 3, delves into the fundamental concepts associated with the proposed model, followed by the discussion of related work in Section 2. Section 4 delineates the proposed model. The following sections provide an explanation of the implementation and evaluation metrics in Section 5, and results analysis and comparison in Section 6. Subsequently, Section 7 present the discussion. Lastly, the paper is concluded in Section 8, which also emphasizes the need for further research.

2.0. RELATED WORKS

This section discusses related work addressing the issue of access control in the security of BYOD (Bring Your Own Device). The literature review is divided into primary categories, based on challenges: authentication rules access control in the tactical layer, risk access control policy in the strategic layer, and policy management and administration in the access control based operational layer.

Bello and colleagues confirmed in [8] that secure BYOD access control should include three layers of security policy, as illustrated in Fig.1. The first layer, the operational layer, handles policy management, service-level agreements (SLAs), user and device registration. The second layer, termed the tactical layer, is predicated on authentication to forestall unauthorized access and safeguard the confidentiality of communication between the BYOD user and the corporate network and resources. Furthermore, policy mechanisms implemented in this layer may provide confidentiality and authenticity for the BYOD environment, thereby satisfying two privacy requirements. The third and final layer, known as the strategic layer, comprises a risk access control policy and monitors attacks to detect and prevent them using IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) techniques, safeguarding user privacy and the company network. Moreover, this layer furnishes attack detection, satisfying security and privacy requirements. Subsequent sections review previous work, based on the security policy layer, and identify limitations in each layer.

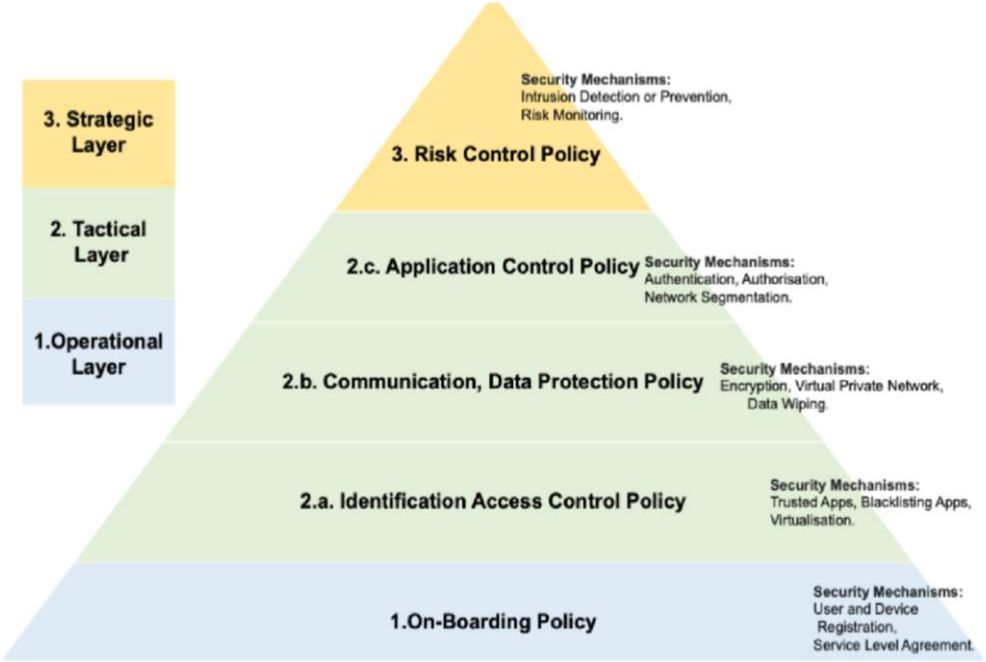


Fig. 1. Secure Three-Layer Architecture for BYOD Access Control Policy.

2.1. Based Authentication Rules and Policies (Tactical Layer)

This section concisely overviews pertinent research on access control strategies for Bring Your Own Device (BYOD), emphasizing the tactical layer. In a BYOD environment, a range of methodologies are employed to establish authentication regulations and rules to mitigate unauthorized access and privacy issues concerning access control. In their study, Lee et al. [4] introduced a novel access control approach that relies on Mobile Device Management (MDM) to ascertain the eligibility of a BYOD for accessing an organizational network. This method operates by evaluating a fixed control policy. Yanson [9] implemented access control integration by utilizing WPA2-Enterprise authentication in educational networks that employ BYOD policies. In their study, Gkamas et al. [10] proposed a robust access control policy for the Greek School Network. This policy considers the user's identity as a determining factor for granting network access. The authors focused on static policy considerations, specifically emphasizing identity as a critical criterion for access control. In their study, Oluwatimi et al. [11] introduced a context-aware access control system that utilizes proximity as a basis. The authentication process involves the use of a time-dependent challenge-response technique. Biometric authentication in BYOD devices effectively evaluates users' behavioral and physiological characteristics by leveraging the accelerometer and fingerprint sensors. This approach relies solely on context-based biometrics for user authentication. Seneviratne and Senaratne [12] conducted a study wherein they implemented access control policies founded on fine-grained network and mobile device security policies. These policies were integrated with pre-existing authentication systems to effectively govern mobile device access and network services for individuals, groups, or devices.

These strategies involve researchers emphasizing improving access control rules by integrating static factors, such as identification or fingerprint verification, into making access decisions. This integration aims to limit the access permissions granted to BYOD users when accessing protected resources. Nevertheless, the utilization of authentication based fixed policies may decrease the dynamism and flexibility of access control, thereby prolonging the implementation of access decisions and making the system more susceptible to attacks. In addition, it is essential to note that these proposed solutions may still allow for unauthorized access. Therefore, it is crucial to consider the potential changes in access behavior exhibited by BYOD users when utilizing resources. This can be achieved by establishing policies based on dynamic attributes, including time and location, as well as real-time risk factors.

2.2. Based Attack Detection and Risk Access Control (strategic layer)

Numerous solutions have been devised to mitigate insider risks in Bring Your Own Device (BYOD) environments, leveraging behavioral models and anomaly detection techniques. Kim and Lee [13] proposed a network-based risk identification tool incorporating a machine learning algorithm. This tool aims to identify and assess malware present on mobile devices that are infected under the BYOD policy. Nevertheless, this particular approach is unsuitable for applications that use log files. Aldini and colleagues [14] proposed an improvement to an existing method that utilizes an OPPRIM-based risk policy model to detect denial of service attacks, probe attacks, and torrent traffic in BYOD environments. This enhancement provides an adaptable, flexible, and cost-effective approach. In their study, Ammar et al. [15] introduced a framework for malware detection in Android BYOD devices using a classification-based approach within the context of Software-Defined Networking (SDN). Their proposed technique establishes a self-adaptive network that safeguards essential services and mitigates internal attacks. However, it is suggested that further enhancements and extensions are necessary to enable the detection of Advanced Persistent Threats (APTs).

Furthermore, Ali et al. [16] introduced a risk-based access control model incorporating a dynamic risk estimation technique. This approach utilizes various features to assess the security risk associated with each access request. The algorithm assesses access privileges by considering user context, resource sensitivity, action severity, and risk history. The technique under evaluation should encompass a comprehensive ecosystem that spans from the beginning to the end. Zungur and colleagues [17] proposed a conceptual framework that utilizes artificial neural networks (ANN) and data mining techniques to identify abnormal behavior and unauthorized access in BYOD environments. The primary objective of the research conducted by Alghamdi et al. [18] was to detect abnormal activities exhibited by BYOD devices connected to a corporate platform. Subsequently, the study employed an intelligent filtering technique to subject these devices to the Access Control and Security Management (ACSM) system for platform authorization. This approach enables the establishment of end-user access control policies and serves as a safeguard against potentially harmful mobile applications. However, conducting security testing becomes increasingly complex when applications are subjected to persistent attacks.

Yin et al. introduced a risk-based access control framework incorporating a multilayer perceptron (MLP)-based intrusion detection system. This system utilizes a novel hybrid feature selection technique called IGRF-RFE. The IGRFRFE approach consisted of a combination of filter feature selection and wrapper feature selection techniques. According to Yin et al. [5], the study’s findings revealed that the accuracy of multi-classification for the MLP model improved from 82.25% to 84.24%. Furthermore, Han et al. [6] introduced a novel access control system called the Intrusion Detection Hyperparameter Control System (IDHCS). This system effectively manages and trains a deep neural network (DNN) feature extractor and a k-means clustering module through PPO-based reinforcement learning techniques. The Intrusion Detection and Host-based Cybersecurity System (IDHCS) effectively manages the Deep Neural Network (DNN) feature extractor to extract the most significant network features. It employs the k-means clustering algorithm in conjunction with the UNSW-NB15 dataset to accurately detect intrusions, achieving a commendable accuracy rate of 0.94268. In their study, Bhardwaj et al. [7] proposed a novel risk access control model that integrates a well-defined stacking sparse autoencoder (AE) for feature learning with a deep neural network (DNN) for the classification of network traffic into benign or DDoS assault traffic using the Naive Bayes algorithm. The achieved accuracy of the model was 0.824. Additionally, the support vector machine algorithm was employed in this model, which yielded an accuracy of 0.755.

The aforementioned solutions enhance risk access control policies; however, the methodology is constrained to a single layer (the strategic layer) and needs to consider the tactical layer of security BYOD policies for a comprehensive security access model. Furthermore, the study revealed low attack detection accuracy in these solutions. Additionally, the researchers did not sufficiently focus on prediction time and detection accuracy. Therefore, it should be monitored in real-time for anomalous behavior to enhance risk and anomaly detection in access control. Enhanced methods are needed to improve detection accuracy in a short prediction time.

2.3. Based Policy Management and Administration in Access Control (Operational Layer)

To effectively integrate intermediate access modifications, the current policy administration for access control should be revised. The execution of this task presents system administrators with challenges and is susceptible to errors, such as over-privileged access, which can be attributed to the lack of appropriate tools [19]. The system is exposed to potential cybersecurity risks because of the labor-intensive and error-prone process of manually updating policies [20]. The identification of such threats or misconfigurations in an expedient manner can result in substantial security incidents. A methodology framework has been suggested for the automation of policy administration processes.

A novel access control approach that employs machine learning was introduced in the study conducted by Argento et al. [20]. This method demonstrates the ability to dynamically update policies during runtime, thereby effectively mitigating potential security dangers. The proposed solution is designed to monitor and acquire knowledge regarding behavioral access attributes, including user location, data volume, and access frequency. Subsequently, this contextual knowledge is employed to modify existing access control regulations. The authors implemented the method by integrating a novel component into the policy management point (PAP) of the access control system to denote its contextual behavior. The innovative component is intended to generate user profiles by analyzing and monitoring their access patterns. Subsequently, these profiles are implemented to establish access control policies.

In addition, Alkhresheh and colleagues [21] introduced an adaptive system that was specifically designed for the deployment of the Internet of Things (IoT). The objective of this system is to dynamically optimize access restrictions in accordance with the access behaviors of IoT devices. Furthermore, the authors suggest the integration of a taxonomy policy management module that includes an access behavior classifier and policy optimization components, as well as access policy adaptation functionalities.

PAMMELA, a machine learning-based approach for managing Attribute Based Access Control (ABAC) policies, was also introduced by Gumma et al. [22]. PAMMELA develops revised regulations and improves preexisting policies by integrating them in response to the proposed modifications. By acquiring rules from an existing policy in a system that exhibits similar characteristics, the proposed solution, PAMMELA, can generate novel policies for a given system. The initial phase of the proposed approach is dedicated to instructing the supervised machine learning classifier with the norms of the Attribute-Based Access Control (ABAC) policy. This solution is a two-phase solution. Subsequently, the system presents a sequence of access requests to the classifier that has undergone training during the second phase. Subsequently, it generates a set of rules, each of which is derived from the access decision made by the classifier for its respective request.

2.4. Related Work Evaluation Summary

Based on the challenges in BYOD security and access control, related work is divided into three primary categories: authentication policy-based access control, risk policy-based access control, and policy management and administration in access control. The study discovered that some researchers focused on access control techniques that rely on fixed attributes for access decisions rather than taking dynamic attributes such as risk access request behavior into account in real-time, which may be negative in dynamic access control. In addition, other researchers concentrated on risk access control employed by behavioral models and anomaly detection techniques to prevent cyberattacks and unauthorized access without considering the other security policy layers. Furthermore, the study discovered that risk access control solutions provide effort into attack detection techniques but are limited to one single layer and need to improve performance accuracy in real-time prediction time. Additionally, it should extend the anomaly detection algorithm to include real-time adaptive adjustment policy management. This paper aims to critically examine existing access control mechanisms in the context of the layered security approach to

BYOD (Bring Your Own Device) policies. It will evaluate whether these mechanisms meet the necessary security conditions for BYOD environments, including all security policy tiers: Operational, Tactical, and Strategic. The studies will be evaluated based on the following criteria: the efficacy of solutions at any security layer, considering dynamism, real-time capabilities, attack detection, and policy adaptability, as depicted in the Table 1. The subsequent points will provide an explanation of the work evaluation criteria for secure access control in the BYOD environment.

Table 1. Evaluation of Existing Access Control Approaches (Related Work)

Ref	Operational Layer	Tactical Layer	Strategic Layer	Dynamic	Real Time	Attack Detection	Adaptive Policy
[4]	✗	✓	✗	✗	✗	✗	✗
[5]	✗	✗	✓	✓	✗	✓	✗
[6]	✗	✗	✓	✓	✗	✓	✗
[7]	✗	✗	✓	✓	✗	✓	✗
[9]	✗	✓	✗	✗	✗	✗	✗
[10]	✗	✓	✗	✗	✗	✗	✗
[12]	✗	✓	✗	✗	✗	✗	✗
[13]	✗	✗	✓	✓	✗	✓	✗
[14]	✗	✗	✓	✓	✗	✓	✗
[15]	✗	✗	✓	✓	✗	✓	✗
[16]	✗	✗	✓	✓	✗	✓	✗
[18]	✗	✗	✓	✓	✗	✓	✗
[19]	✓	✗	✗	✓	✗	✓	✗
[21]	✗	✗	✗	✓	✓	✓	✓
Our work	✓	✓	✓	✓	✓	✓	✓

- **Operational Layer:** This layer guarantees that the access control model considers management policy concerns. The administrative effort and the necessity for manual updates are minimized by the adaptive management of policies in accordance with the current status of access requests.
- **Strategic Layer:** This layer guarantees that the identities of BYOD (Bring Your Own Device) users are sufficiently monitored and verified, thereby fostering trust between BYOD users, organizations, and their resources. Strategic Layer: This item is a strategic layer. This layer ensures that assaults associated with BYOD devices are effectively identified and mitigated.
- **Dynamic Policy:** This policy type generates decisions on access requests based on dynamic, real-time attributes such as time, location, and risk, rather than solely on static policies like identity.
- **Real-time:** Decisions within the access control system are made based on the real-time behavior of the access request, emphasizing the critical role of "real-time" in access control security.
- **Performance:** The technology used to detect attacks in the strategic layer must be capable of attaining high accuracy and rapid prediction times in order to effectively counteract attacks.
- **Adaptive Policy:** require dynamic and flexible modifications. In instances of anomalous access request behavior, policies should dynamically adjust to correspond with the characteristics of the request.

3.0. FOUNDATIONAL CONCEPTS AND TERMINOLOGIES

This section discusses the basic concepts of the paper.

3.1. Basic Terminology

BYOD Security Policy: According to Bello and colleagues in [8], policies that consist of three layers are necessary for security in a BYOD environment. The security policy must be divided into three categories, as illustrated in Fig. 1, in order to ensure secure BYOD access control. The Operational Layer is the first layer, and it is responsible for the management and administration of policies. The Tactical Layer, which is the second layer, includes dynamic policies and authentication mechanisms. The Strategic Layer is the final layer, which prioritizes the real-time detection and monitoring of hazards. This is an optimal security policy for comprehensive access control in a BYOD environment.

Dynamic Policy: is a security method that aims to enhance access control by including real-time and dynamic access attributes in the determination of access rights. Unlike traditional access control systems that primarily depend on static rules, such as identity-based access control, dynamic access control incorporates factors such as time, location, and risk to determine whether a user or entity should be granted access to a specific resource or system.

Risk Monitoring: assesses access requests through real-time risk evaluation. Ongoing surveillance and immediate detection of threats during access requests in real-time mitigate vulnerabilities and deficiencies in BYOD (Bring Your Own Device) settings and bolster user privacy. Realtime monitoring is essential for maintaining access control security.

Adaptation Policies: Access control encompasses adaptive policies, signifying dynamic and flexible adjustments to address the nature of the request in instances of anomalous access request behavior. This alleviates the responsibility of system administrators in overseeing control rules, liberating them from human mistake and bolstering the security of access control against possible vulnerabilities and assaults.

Machine Learning Methodologies: The proposed system uses machine learning techniques for anomaly detection algorithms and assesses their effectiveness in swiftly predicting attacks. The goal of using machine learning methodologies is to improve access decisions by making them more precise, adaptive, and responsive to evolving security threats.

3.2. Attributed Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) is a methodology that utilizes attributes and policies to enforce access rights. ABAC policies may employ properties including environment, user, resources, and objects. The suggested access control utilizes a Boolean policy expression, incorporating "if, then" stipulations for the user (the access requester), the resource (the organization’s network and assets), and the procedure. For example, if the requester is an administrator, grant access control read and write access to sensitive information. While there are differences in Role-Based Access Control (RBAC) [23], which uses policies as predefined roles, the main difference between RBAC and ABAC is that policies represent a complex set of logical rules. ABAC policies are selected due to their ability to govern access based on a range of attributes, such as subject, resource, and environmental attributes. The system offers a high degree of flexibility in articulating overarching access control requirements by integrating multiple access control policies and accommodating specific business access control needs. The fundamental components of access control model encompass the subsequent elements:

- Policy Administration Point (PAP): Create and manage policies, policy sets, and access policies specified by the policy administrator.
- Policy Decision Point (PDP): Evaluate if access requests are permitted, evaluate the available policies, and make authorization decisions.
- Policy Enforcement Point (PEP): Implements access determinations received from PDP. Receive and send messages; interact with external applications based on results and obligations; that is a directive from the PDP to the PEP about what actions must be taken before and after access is granted.
- Policy Information Point (PIP): Delivers information regarding subject, resource, and environmental attributes.
- Context Handler (CH): Convert the access request and forward it to the Policy Decision Point (PDP).
- Subject (S): BYOD user performing an action on a resource.
- Resource (R): The information, services, and system elements supplied to the user by the organizational system.

4.0. PROPOSED MODEL

This section delineates the proposed access control model, as illustrated in Fig.2. For effective policy administration, it is composed of three essential components: adaptive policy adjustment, real-time risk monitoring, and dynamic policies. Further details regarding each element of the proposed methodology are provided in the subsequent subsections. Consequently, the proposed solution is distinguished by several core characteristics:

- **Dynamic Risk-Based Access Decision Making:** The access decisions in the proposed model are determined by taking into account real-time environmental variables. A critical attribute is evaluating the potential security risk associated with each access request. The framework employs this attribute to make well-informed decisions regarding resource access. In addition, it continuously monitors behavioral patterns to optimize access control rules. Integrating machine learning algorithms allows for the precise tuning of policies by identifying unusual or anomalous user behaviors.

- **Enhanced Threat Detection and Access Control:** This component substantially enhances insider threat detection and improves access control. The solution generates permission access decisions based on the characteristics of attribute-based access control. It is an authorization model that is context aware, risk-sensitive, and dynamic and adjusts to real-time conditions to access corporate resources. The approach ensures regulatory compliance by implementing dynamic access control policies with precisely defined authorization attributes. Implementing this methodology will increase the organization's control flexibility using its existing infrastructure.

These components function synergistically to establish a secure and efficient framework for enforcing access decisions and managing access permissions, which can adapt dynamically to changing environmental conditions and threats.

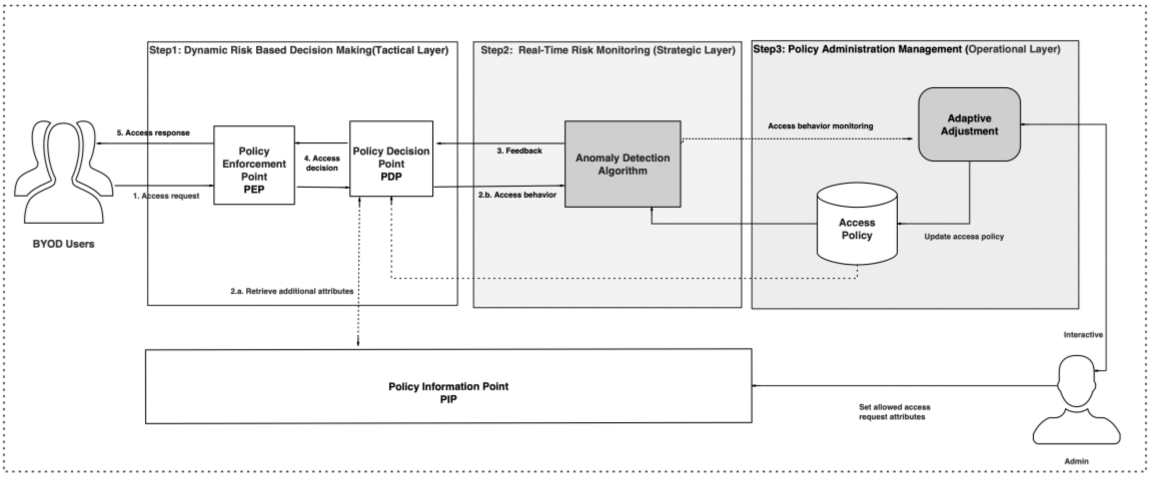

Step1: Dynamic Risk Based Decision Making(Tactical Layer)
Step2: Real-Time Risk Monitoring (Strategic Layer)
Step3: Policy Administration Management (Operational Layer)
5. Access response
1. Access request
BYOD Users
Policy Enforcement Point PEP
4. Access decision
Policy Decision Point PDP
3. Feedback
2.b. Access behavior
Anomaly Detection Algorithm
Access behavior monitoring
Adaptive Adjustment
Access Policy
Update access policy
2.a. Retrieve additional attributes
Interactive
Policy Information Point PIP
Set allowed access request attributes
Admin

Fig.2. Three-Layer Approach to BYOD Security: Utilizing Machine Learning Techniques.

4.1. Step 1: Dynamic Risk-Based Decision Making

This element is essential for the management of model dynamics by integrating dynamic policies into the access control framework. It is specifically designed for intricate environments, such as Bring Your Own Device (BYOD). Additionally, our proposed solution is based on dynamic risk attributes, in contrast to previous solutions that relied on static attributes such as identity or role. Furthermore, it makes access decisions based on dynamic risk attributes that define conditions under which access to a resource is permitted or denied based on the risk attribute. The policy includes two rules:

- **DynamicRiskBasedRule:** This rule incorporates a condition to evaluate the normalcy of the risk level in access request attributes, which are generated through machine learning. When this criterion is met, the rule's effect is marked as 'permission,' indicating authorized access. Specifically, an access decision is granted when the output from the machine learning engine, connected to the policy decision engine, is zero. This zero output indicates the absence of any specified attack types in the access request attributesnamely, Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms thereby justifying read access to the objects.
- **DefaultDenyRule:** If the conditions stipulated in the DynamicRiskBasedRule are not met, this rule activates the 'deny' effect, establishing a default decision to restrict access. In our scenario, access is denied by default if the result from the machine learning engine associated with the policy decision engine is one, indicating the presence of an anomaly.

4.2. Step 2: Real-Time Risk Monitoring and Anomaly Detection

The second component of our suggested access control approach is a risk and anomaly detection module, which enhances the system by facilitating simultaneous access requests and identifying possible security risks. The algorithms employed identify distinct features in anomalous access requests that deviate from established norms. In highly complex and dynamic environments characterized by a high volume of access requests that vary across multiple dimensions, the efficacy of this approach is essential. Furthermore, the suggested technique implements four strategic algorithms in access decisions that depend on risk monitoring and anomaly detection, as illustrated in Fig. 3 including distributed-based algorithms, density-based algorithms, statistical-based algorithms, and neural network-based algorithms. The theoretical application of these algorithms within an access control scenario is further elaborated upon in the subsequent section, mainly focusing on detecting attacks and monitoring risks.

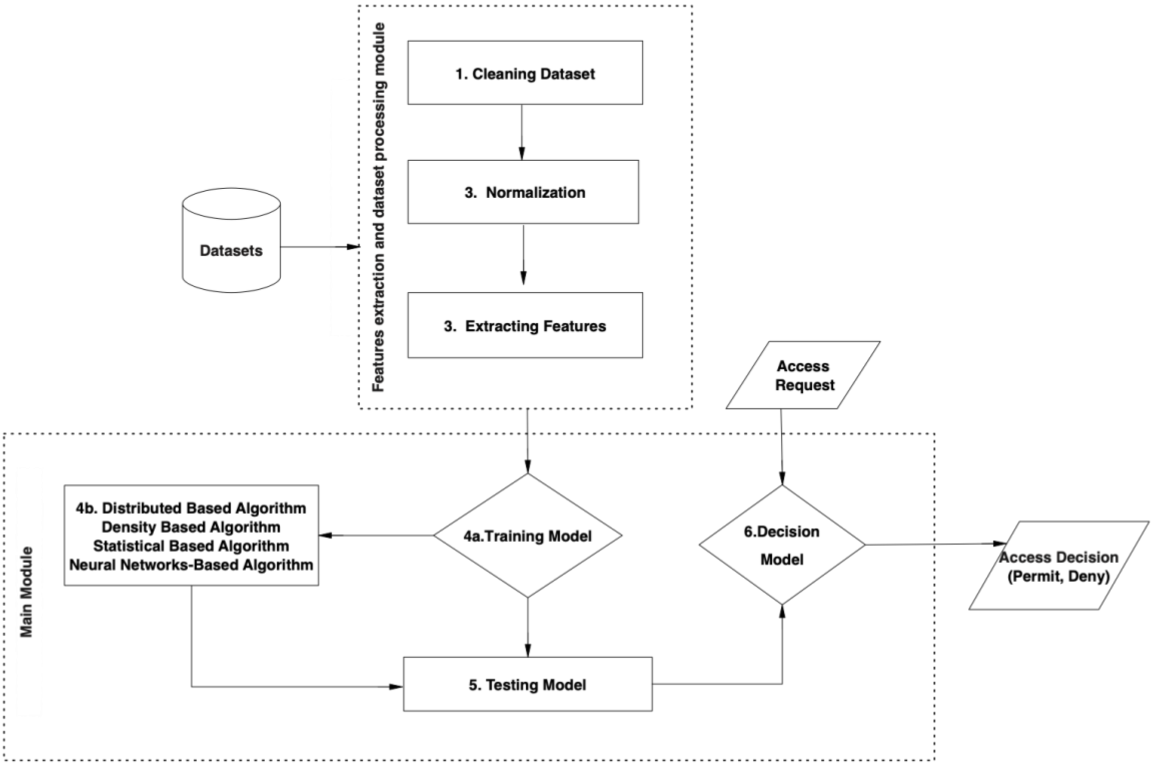

Features extraction and dataset processing module
1. Cleaning Dataset
3. Normalization
3. Extracting Features
Datasets
Access Request
Main Module
4b. Distributed Based Algorithm
Density Based Algorithm
Statistical Based Algorithm
Neural Networks-Based Algorithm
4a.Training Model
6.Decision Model
Access Decision (Permit, Deny)
5. Testing Model

Fig.3. Access Decision Based on Risk Monitoring and Anomaly Detection using a Machine Learning Model.

4.2.1. Distributed-Based Algorithm

Distributed-based techniques, such as Random Forest (RF), create decision trees using randomized splitting and resampling. Regarding access requests in access control, RF algorithms define events (access requests) as normal or abnormal by combining decisions from many trees. Its concurrent training on datasets makes RF more resilient, adaptive, and effective in anomaly detection. Furthermore, including the random forest approach in access control encourages transitioning to a distributed paradigm that makes access decisions across numerous nodes. This move improves scalability, flexibility, and efficiency by streamlining decisions and removing performance bottlenecks in policy decision points. Furthermore, including the random forest approach in access control encourages transitioning to a distributed paradigm that makes access decisions across numerous nodes. This move improves scalability, flexibility, and efficiency by streamlining decisions and removing performance bottlenecks in policy decision points. Moreover, this algorithm dispersed nature significantly improves fault tolerance and adaptability. Therefore, access decision enforcement-based RF technology may enable dynamic and distributed permission determination architectures, which increases its usefulness in complex access control situations. The Random Forest algorithm has some characteristics are as fellow:

- Cascade and Distributed Architecture: The sequential execution of sub-permission engines allows for cross-domain data access. RF Algorithms are educated on policy data.
- Conditional Structure: A combined structure restricts sub-permission engines depending on circumstances, enabling autonomous operation.
- Parallel Architecture: The simultaneous functioning of sub-authority engines removes dependencies and effectively handles concurrent access request.

Random forest (RF) enhances security risk predictions by capturing complex relationships and identifying deviations. To sum up, this technology in security access control offers a versatile solution to the ever-changing nature of threats. The classification decision procedure can be mathematically expressed as follows:

$$H(X) = \arg\max_{Y}\left(\frac{1}{N}\sum_{i=1}^{N} P(h_i(X) = Y)\right) \tag{1}$$

where X and Y represent a single classification sample and its corresponding classification target, respectively. Classification results for the i-th tree are represented by $h_i(X)$. The classification result for the i-th tree is represented by the probability function $P(h_i(X) = Y)$. $H(X)$ represents the final classification outcome that was obtained from the Random Forest algorithm. The subsequent section outlines the procedural steps of the algorithm within our proposed approach:

- Define the access control problem and prepare the dataset. In this instance, we employ the UNSW-NB15 dataset, emphasizing the 'attack_cat' attribute, which denotes nine distinct types of attacks. Denote the feature space X, the set of possible outcomes Y, training dataset D, and the number of decision trees T.
- Implement the Random Forest algorithm with a risk policy for access control following these steps:
- Employ a random sampling approach with replacement N to extract data points from the training dataset D and generate bootstrapped datasets N.
- Construct a decision tree for each bootstrapped dataset by iteratively expanding nodes using a random subset of features at each split, where F is the full set of features. The methodology is mathematically expressed as follows:

$$F_s \subset F, \quad |F_s| = m, \quad m \ll |F| \tag{2}$$

- Combine predictions from individual decision trees through majority voting, using it as the classification criterion to consolidate the aggregated outcomes. The expression for Random Forest prediction is as follows, where $y\hat{}^{t}(x)$ is the prediction of the t-th decision tree.

$$\widehat{y_{\mathrm{RF}}}(x) = \mathrm{MajorityVote}\left(\{\widehat{y^t}(x)\}_{t=1}^{T}\right) \tag{3}$$

- For a new access attempt with feature vector x_{new}, obtain the prediction from the Random Forest:

$$\widehat{y_{\text{new}}} = \widehat{y_{\mathrm{RF}}}(x_{\text{new}}) \tag{4}$$

- For access decision-making, incorporate the risk policy and the RF algorithm into the access control decision point (PDP engine).
- Create a decision rule that maps the predicted risk level $y\hat{}_{\text{new}}$ to access control decisions, such as granting or denying access.

$$\text{Access Decision} = \begin{cases} \text{Allow Access,} & \text{if } \hat{y}_{\text{new}} \leq \text{Threshold} \\ \text{Deny Access,} & \text{otherwise} \end{cases}$$

4.2.2. Density-Based Algorithm

The K-Nearest Neighbors (KNN) algorithm is particularly effective in risk monitoring and access control among density-based algorithms because of its capacity to efficiently identify patterns and anomalies within datasets. KNN is a statistically based algorithm that employs proximity metrics to classify access request patterns, making it an ideal candidate for identifying potential security threats. Making real-time access decisions and adapting to changing surroundings strengthens risk management systems. Organizations can apply a security and dynamic access control policy approach by incorporating KNN, increasing overall resilience, trust, and privacy, and responding quickly to emerging security risks. The K-nearest neighbors (KNN) technique is a non-parametric strategy predicated on neighborhood-based assessment. This approach facilitates categorization without relying on any assumptions regarding the underlying function, which is denoted as $y = f(x_1,x_2,...,x_p)$, and denotes the correlation between the dependent variable and the independent variables [24]. A mathematical formula can be used to characterize the K-Nearest Neighbors algorithm in the context of risk detection and access control:

$$\widehat{y_{\text{new}}} = \text{RiskAggregation}\left(\{\text{y}_\text{i}\}_{\text{i}=1}^{\text{k}}\right) \tag{5}$$

Where the risk level of the i-th nearest neighbor is denoted by y_i, and *RiskAggregation* is a function that is intended to aggregate risk levels using a weighted mean. The proposed approach incorporates the following procedures for the technical implementation of the KNN algorithm:

- Training dataset comprises security categories y_i and features x_i.
- Define the feature space X, set of possible outcomes Y, training dataset D, and the number of neighbors k.
- develop the KNN algorithm with a risk role in access control:
- determine a distance metric $d(x,x')$ to quantify the similarity between feature vectors in access request x and x' in the feature attribute space. – Based on the measured distances, determine the k nearest neighbors.
- The security level of the new access request attempt should be determined by the majority or weighted vote of the security levels of its k nearest neighbors.

$$\widehat{y_{\text{new}}} = \text{Vote}(\{y_i\}) \tag{5}$$

- Integrate the risk rule and the KNN algorithm into the regulation's access decision at the policy decision point (PDP engine) to facilitate access decision enforcement.
- Determine a decision rule that maps the predicted risk level $y\hat{}_{\text{new}}$ to access control decisions. For instance, permit access if $y\hat{}_{\text{new}} \leq$ Threshold, but deny access otherwise.

$$\text{Access Decision} = \begin{cases} \text{Allow Access}, & \text{if } \hat{y}_{\text{new}} \leq \text{Threshold} \\ \text{Deny Access}, & \text{otherwise} \end{cases}$$

4.2.3. Statistical Based Algorithm

The Histogram-Based Outlier Score algorithm is utilized in the study for risk-based access control. This algorithm was selected due to its durability, scalability, efficiency, and proficiency in detecting anomalies and noise resilience. HBOS is an appropriate statistical algorithm for security access control and risk monitoring due to these characteristics.

Additionally, HBOS uses a univariate histogram to identify abnormal access for each feature in an access request. The estimated density is represented by the height of a histogram for each data feature [25], as defined by Equation 7. In order to guarantee that each feature contributes equally to the anomaly score, each histogram is normalized to a maximum height of 1.0. Consequently, the HBOS of each data sample p is determined by the height of the bins in which the sample is located.

$$H(X_i) = \{h_1, h_2, \dots, h_k\} \tag{7}$$

in which $H(X_i)$ denotes the histogram for feature X_i, and h_j is the height of the j-th bin. When computing the HBOS for a particular data sample p, the strategy employs the bin heights that correspond to the bins in which the data set is situated. For a sample p, the HBOS score is calculated as follows:

$$\text{HBOS}(p) = \sum_{i=1}^{d} \quad \log\left(\frac{1}{H'(X_i)[\text{Bin}(p,X_i)]}\right) \tag{8}$$

where *d* denotes the number of features, Bin(*p,X$_i$*) signifies the bin index of sample *p* within the histogram of feature *X$_i$*, and log refers to the natural logarithm. The subsequent steps delineate the application of the algorithm in the suggested methodology:

- Arrange the data consistent with the risk-based access control approach to the suggested strategy. Include any pertinent parameters for HBOS, denote the feature space as *X*, the set of possible results as *Y* , and the training dataset as *D*.
- Execute the HBOS procedure with a risk feature for access control by adhering to the following steps:

1. Distribute the feature space into segments and generate histograms foreach dimension. The frequency of data elements falling into each bin is denoted by the height of the bin.
2. Utilize the histograms to determine the outlier score for each data point.The score is calculated by multiplying the inverses of the bin heights for each dimension.

$$\text{Outlier Score}(x_i) = \prod_{j=1}^{n} \frac{1}{h_j(x_{i,j})} \tag{9}$$

where x_i is the *i*-th data point, *n* is the number of dimensions, and $h_j(x_{i,j})$ is the height of the bin corresponding to the *j*-th dimension corresponding to the *i*-th data point.

3. Assess the aggregate risk level for each access request point by aggregating the outlier scores, considering all dimensions.
4. Predicting a new access attempt involves assigning risk attributes to the new access attempt based on the risk attributes identified in the experimental scenario. These risks are represented by the nine attack attributes, which indicate abnormal access. ($y\hat{}_{\text{new}}$).

- Incorporate the HBOS algorithm with the risk policy into the policy access control decision-point (PDP engine) for access decision-making.
- Define a decision rule to map the predicted risk level $y\hat{}_{\text{new}}$ to access control decisions. For example, allow access if $y\hat{}_{\text{new}} \leq$ Threshold, otherwise deny access.

$$\text{Access Decision} = \begin{cases} \text{Allow Access,} & \text{if } \hat{y}_{\text{new}} \leq \text{Threshold} \\ \text{Deny Access,} & \text{otherwise} \end{cases}$$

4.2.4. Neural Networks-Based Algorithm

The research employs Convolutional Neural Network to enhance risk-based access control systems. This is achieved by extracting features for risk monitoring and anomaly detection. The analysis is based on access control systems. The ability of CNNs to process access requests across multiple layers allows them to autonomously learn intricate feature hierarchies from user behavior and make precise access decisions without the need for substantial manual input; this functionality is essential for identifying patterns that indicate unauthorized access attempts.

Moreover, the architectural efficiency of CNNs enables parallel processing, rendering them optimal for real-time analysis and guaranteeing that potential security hazards are promptly addressed. In addition, the adaptability of CNNs enables them to be customized to suit specific security scenarios, thereby increasing their efficacy across a diverse array of systems with minimal retraining. As a result, these attributes collectively reinforce the decision to employ CNNs as an accurate instrument for dynamically confronting emergent threats and sustaining high security levels in access control frameworks. Typically, the architecture of a CNN comprises the following components:

- Utilize learnable filters on the input to capture spatial hierarchies.
- Utilizes the ReLU activation function to introduce non-linearity, thereby enabling the network to learn complex patterns.
- Minimize the spatial dimensions of the representation to enhance computational efficiency.
- Classify outputs via fully connected layers to ascertain the probability of each access request category.

The mathematical explanation of the convolution process in a convolutional neural network (CNN) is as follows:

$$f(x) = \mathrm{ReLU}(W * x + b) \tag{10}$$

In this context, W denotes the weights of the filters, $*$ represents the convolution operation, x indicates the input, and b signifies the bias. The integration process comprises the following components:

- Standardize the input data to achieve consistency for the convolutional neural network. This includes normalizing the data to a range appropriate for the activation functions employed in the network.
- Utilize labeled data to train the CNN, modifying the weights via backpropagation to reduce error in classification.
- Following anomaly detection, the CNN assesses the access decision using a decision score.
- Integrate the CNN algorithm into the policy decision-point (PDP engine) in access control to facilitate access decision-making.
- Establish a decision rule to correlate the result score of the CNN with access control determinations.

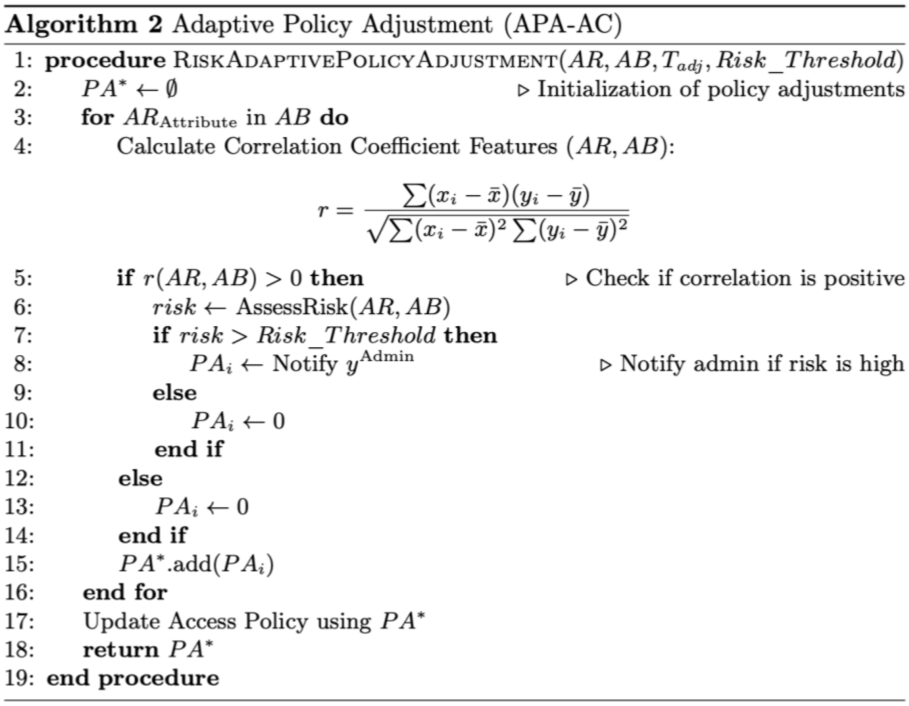
$$\text{Access Decision} = \begin{cases} \text{Allow Access Request,} & \text{if CNN Score} > \text{Threshold} \\ \text{Deny Access Request,} & \text{otherwise} \end{cases}$$

The score is obtained through the application of the max function in the final fully connected layer of the convolutional neural network (CNN).

$$\text{CNN Score} = \mathrm{softmax}\left(W_{fc} \cdot y + b_{fc}\right) \tag{11}$$

In this context, W_{fc} and b_{fc} represent the weights and bias of the fully connected layer, while y denotes the output from the preceding layer.

4.3. Step 3: Adaptive Policy Adjustment for Policy Management



Algorithm 2 Adaptive Policy Adjustment (APA-AC)

```
procedure RiskAdaptivePolicyAdjustment($AR, AB, T_{adj}, Risk\_Threshold$)
    $PA^* \leftarrow \emptyset$                         ▷ Initialization of policy adjustments
    for $AR_{\text{Attribute}}$ in $AB$ do
        Calculate Correlation Coefficient Features ($AR, AB$):
            $r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}}$
        if $r(AR, AB) > 0$ then                     ▷ Check if correlation is positive
            $risk \leftarrow$ AssessRisk($AR, AB$)
            if $risk > Risk\_Threshold$ then
                $PA_i \leftarrow$ Notify $y^{\text{Admin}}$          ▷ Notify admin if risk is high
            else
                $PA_i \leftarrow 0$
            end if
        else
            $PA_i \leftarrow 0$
        end if
        $PA^*$.add($PA_i$)
    end for
    Update Access Policy using $PA^*$
    return $PA^*$
end procedure
```

The objective of this component is to autonomously modify policies in response to identifying anomalies in access requests' behavior using machine learning algorithm to evaluate the attributes and patterns of access requests. This component manages and enforces rules concerning privacy and trust through two phases: adaptive policy modification and risk policy, employing anomaly detection algorithms.

The Adaptive Policy Adjustment method, as delineated in 1, is crucial for the dynamic modification of access control policies. This is achieved by incorporating statistical correlation evaluations based on risk thresholds. The following are the procedural steps:

- Initializes an empty set, *PA*, that holds the policy adjustments calculated by the algorithm.
- Determines the correlation coefficient, *r*, for each attribute in access request data (*AR*) and access behavior metrics (*AB*). Here, x_i and y_i denote the attribute and behavior values, respectively.
- Evaluates risks and enforces access decisions. The method compares the risk of these metrics to a predetermined risk threshold, $Risk_Threshold$, if *r* is positive, indicating a relationship between the cess request and behavior.
- When the risk in the assessment is elevated (surpassing the threshold), the algorithm incorporates a policy modification to alert an administrator, signifying a possible requirement for intervention. If the risk is below the threshold or if *r* is negative, no modifications are implemented.
- Integrates all policy modifications into *PA*. This set is utilized to update the policy on a system-wide approach and is returned for additional actions or evaluations.

Consequently, as delineated in the study, the proposed algorithm employs a sophisticated and adaptive approach to manage access control in response to abnormal access behavior effectively. Dynamic thresholding, its primary feature, enables the real-time calibration of the system's sensitivity to these behaviors by utilizing an adjustment threshold (T_{adj}). Furthermore, the algorithm implements adaptive notification strategies. By analyzing the correlation coefficient (*r*) between abnormal behavior (*AB*) and access requests (*AR*), notifications are exclusively initiated when a positive correlation is identified. This method ensures that notifications are contextually pertinent and meaningful, hence reducing the incidence of superfluous alerts, mitigating alert fatigue, and concentrating on potential security issues. Moreover, the algorithm's policy change method illustrates its versatility. It adaptively reacts to alterations in user behavior patterns by modifying access controls according to the correlation coefficients and the defined adjustment threshold. Consequently, the access control system remains contingent upon the prevailing security conditions, facilitating prompt and efficient decision-making.

5.0. IMPLEMENTATION AND MODEL EVALUATION:

This section explains the implementation of the proposed model, the tool used, and how to evaluate the solution's effectiveness. The author used an iOS Mac with an M1 processor and 16GB of RAM to implement the prototype implementation, as well as the attribute-based access control (ABAC) component [26] and a Python code. The model was modified to include real-time risk monitoring. An adaptive policy adjustment component based on machine learning was also added, and the decision process was adjusted to incorporate the component's feedback. Furthermore, this experiment will utilize a Sketch, which includes all the powerful anomaly detection algorithms required. Finally, we evaluate the effectiveness of attack detection algorithms using the UNSW-NB15.

5.1. Datasets and Feature Selection

We used the UNSW-NB15 dataset [27] to assess our suggested access control model's performance. The data set, which was curated by the Australian Centre for Cyber Security (ACCS), includes real-world network behaviors, artificially manufactured abnormal behaviors, and nine specialized attack categories: backdoors, DOS attacks, fuzzers, generic exploits, shellcode, worms, and reconnaissance. It also includes real-world network behaviors and artificially synthesized anomalous behaviors. It includes 2,540,044 records, each with 49 features, including a class label. Given the dataset's extensive size, we trained and tested the machine-learning model on a subset consisting of 150,000 rows and 194 columns. Initially intended for training intrusion detection systems (IDS) [27], the dataset was repurposed for our access control study, focusing on traffic-related features and excluding attack category features from our training dataset. Consequently, our framework leverages algorithms to detect behaviors that may or may not be indicative of the nine outlined attack types.

The experimental assessment of the suggested mechanism was subsequently conducted using the UNSW-NB15 dataset. A customized partition dataset consisting of 150,000 rows and 194 columns was modified to satisfy the application of anomaly detection based on access control. This subset was further divided into groups for testing and training to guarantee identical distributions across both. Our investigation focused on the "Label" attribute to differentiate between standard (0) and abnormal (1) access requests, with a specific emphasis on traffic-related features and a deliberate omission of attack-related characteristics. This attribute distinguishes between benign "normal" traffic and a "normal" category that encompasses a variety of attack scenarios and identifies the risks associated with nine types of threats. The method of classification is essential for the efficient management of network traffic and the enhancement of security through risk-based access control.

Additionally, we employed the SelectKBest algorithm from the scikit-learn library for feature selection. SelectKBest evaluates the importance of features using a specified scoring function and selects the top K features. In this case, the algorithm identified the top 20 most significant features by setting the K parameter to 20. Subsequently, these attributes served as inputs for our machine learning approach. The technique is particularly beneficial when an algorithm performs well on training data but poorly on unseen data, as it reduces the model's complexity, improves performance, and prevents overfitting. Ultimately, the dataset was divided into two sets: 80% for training and 20% for performance evaluation, which enabled a thorough examination of the model's efficacy in a BYOD environment.

5.2. Evaluation metrics

Accuracy and the AUC-ROC curve are evaluation metrics used to assess performance. Table 2 displays a simplified confusion matrix for classifying results. According to the one versus all principle, there are four general cases in classification tasks involving machine learning:

Table 2. Confusion Matrix

Actual Results	Predicted Results	
	Positive	Negative
Positive	TP (True Positive)	FN (False Negative)
Negative	FP (False Positive)	TN (True Negative)

- True Positive (TP): denotes samples that were accurately classified as positive.
- False Negative (FN): denotes incorrectly classified positive samples.
- False Positive (FP): denotes incorrectly classified negative samples.
- True Negative (TN): denotes samples that were correctly classified as negative.

Accuracy: is the ratio of correctly classified samples to the total number of samples, as determined by Equation 12.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (12)$$

False Positive Rate(FPR): determined by Equation 13, is the proportion of incorrectly classified positive samples to all samples that should have been negative.

$$FPR = \frac{FP}{FP+TN} \quad (13)$$

ROC Curve: The receiver operating characteristic (ROC) curve illustrates the FPR and TPR of the model's predictions at various thresholds. The area under the ROC curve (AUC), as defined by Equation 14 determines the area under the ROC and can be used to evaluate the model's performance.

$$AUC_{ROC} = \int_0 \frac{TP}{TP+FN}\, d\left(\frac{FP}{TN+FP}\right) \quad (14)$$

Prediction Time: indicates the duration required for the system to assess and determine whether a given access request constitutes an anomaly. This metric is of the utmost importance in real-time systems, where prompt decision-making is required to ensure security while minimizing delay. Denote the time at which an access request is received as t_{start} and the time at which a decision is rendered as t_{end}.

$$T_p = t_{\text{end}} - t_{\text{start}} \quad (15)$$

Adaptive Policy Adjustment Accuracy: This metric assesses the adaptive policy's ability to modify access controls by identified risks and anomalies. This feature signifies the system's capability to accurately modify access privileges in response to changing circumstances or detected threats. In order to evaluate precision, the "correct" adjustments N_{ca} are compared to the total modifications N_a about a predetermined set of rules or expected behaviors across multiple scenarios.

$$A_{\text{pa}} = \frac{N_{ca}}{N_a} \quad (16)$$

6.0. RESULTS ANALYSIS

This subsection evaluates the suggested access control policy model's accuracy in terms of detecting attacks, as well as its processing and prediction times. It also assesses the efficacy of the adaptive policy adjustment procedure in modifying access control policy.

6.1. Performance Evaluation of Anomaly Detection Algorithms

This section analyzes four anomaly detection algorithms based on access control: the distributed approach (RF), the statistical approach (HBOS), the density approach (KNN), and the neural network approach (CNN) and compares their performance in terms of accuracy, prediction time, and processing time. The following subsection analyzes these results in detail before and after applying data processing.

6.1.1. Performance Analysis Before Pre-Processing

Anomaly detection algorithms were carefully assessed for their ability to identify anomalous access requests. The evaluation utilized the Area Under the Receiver Operating Characteristic Curve (AUC) as the primary metric. The AUC is a reliable measure of model performance that is scale-independent and immune to classification thresholds, making it advantageous. The subsequent analyses assess the performance of the anomaly detection algorithm both before and after the implementation of the pre-processing technique.
Performance Analysis Before Pre-Processing Analyzing Performance Prior to Pre-processing As indicated by the accuracy metrics in Table 3, the efficacy of algorithms in identifying anomalous access requests within a risk-based access control system was moderate to low prior to the implementation of data pre-processing techniques.

Table 3. Performance of Anomaly Detection Algorithms Before Preprocessing

Methods	Accuracy	Prediction Time(s)	Data Processing (s)
HBOS	0.70	0.04	1.99
KNN	0.50	8.00	51.00
CNN	0.60	0.14	40.0
RF	0.45	0.18	2.00

Furthermore, the histogram-based outlier score (HBOS) approach performed the best during the pre-processing phase, with an accuracy rate of 70%, an estimation time of 0.04 seconds, and a processing time of 1.99 seconds. This highlights the opportunity for accurate anomaly detection within a brief prediction period. On the other hand, the Random Forest (RF) algorithm demonstrated a lower accuracy of 45%. However, it was advantageously equipped with a relatively rapid prediction time of 0.18 seconds and a processing time of 2.00 seconds, suggesting that it is appropriate for scenarios necessitating rapid risk assessments. The K-Nearest Neighbors (KNN) and Convolutional Neural Network (CNN) algorithms achieved accuracies of 50% and 60%, respectively. However, the extended prediction time of 8.00 seconds of the KNN presents substantial challenges in dynamic risk-based settings. In Fig. 4, the ROC curve illustrates that all models exhibit generally low accurate positive rates, underscoring their limited ability to distinguish between normal and anomalous access attempts without effective pre-processing.

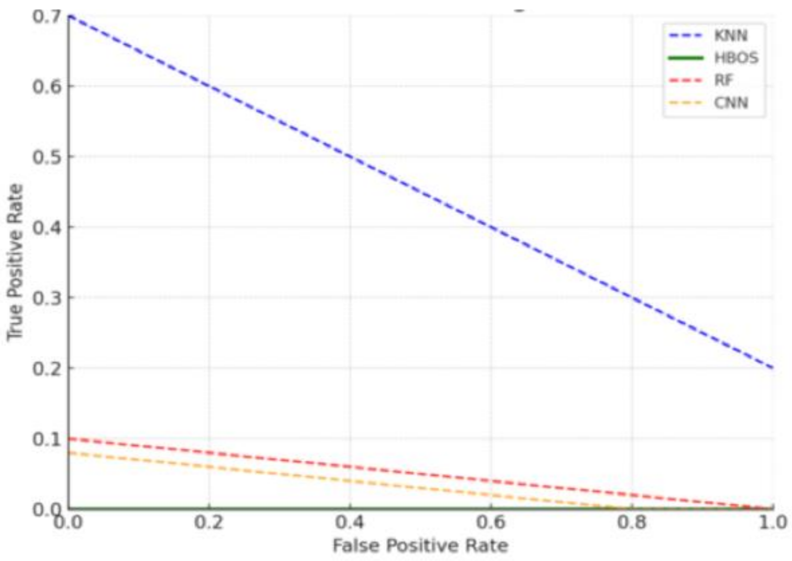


Fig.4. ROC Curve Before Dataset Preprocessing

6.1.2 Performance Analysis After Pre-Processing

The effectiveness of strategies that were employed for anomaly detection-based access control policy was significantly improved by the deployment of pre-processing data techniques, as illustrated in Table 4, mainly with the Random Forest (RF) and K-Nearest Neighbors (KNN) algorithms. The RF algorithm improved to 95% accuracy, reducing prediction time by 0.5 seconds and increasing processing time by 19.00 seconds. This highlights the importance of the pre-processing method. KNN also achieved an enhanced accuracy rate of 94%; however, the corresponding increase in prediction and processing times (129.00 seconds and 523.00 seconds, respectively) may impede its application in situations requiring immediate risk assessments.

Table 4. Performance of Anomaly Detection Algorithms After Preprocessing

Methods	Accuracy	Prediction Time(s)	Data Processing (s)
HBOS	0.46	0.19	5.00
KNN	0.94	129.00	523.00
CNN	0.94	0.9	30.0
RF	0.95	0.5	19.00

In contrast, the HBOS algorithm experienced a minor increase in prediction time to 0.19 seconds, while accuracy decreased to 46% following pre-processing. This decrease suggests that the pre-processing methods employed have an adverse effect, implying that distinct algorithms may require distinct pre-processing strategies to effectively manage risk. Additionally, the ROC curve post-preprocessing demonstrates the improved accuracy of positive rates for Random Forest (RF) and Convolutional Neural Network (CNN) as illustrated in Fig. 5, this validates their exceptional capacity to detect anomalies in the access request accurately.

The above improvements highlight the importance of pre-processing in increasing the efficacy of anomaly detection mechanisms in risk-based access control settings. The significant performance improvements observed in CNN and RF highlight the benefits of data pre-processing in environments where risk-anomaly detection takes precedence. Conversely, HBOS's diminished performance underscores the necessity of customizing pre-processing strategies. This necessity is further exemplified in Fig. 6, which compares the performance of these algorithms prior to and following data processing.

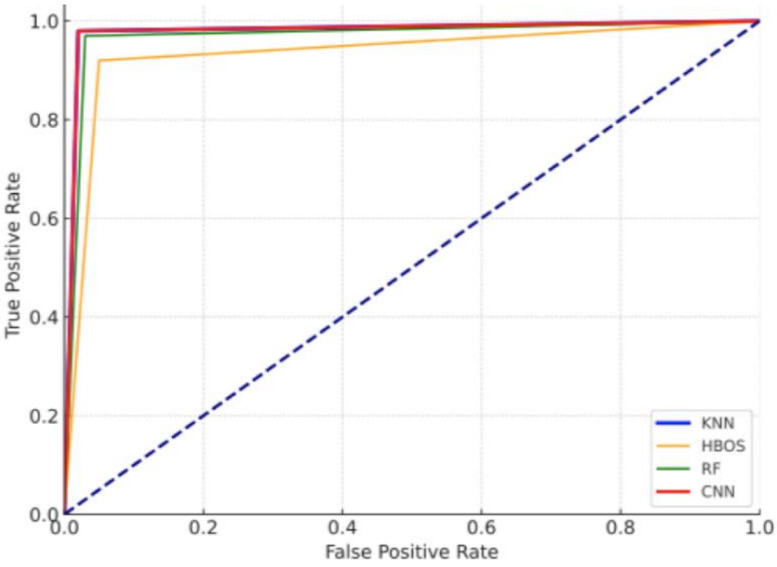


Fig.5. ROC Curve After Dataset Preprocessing

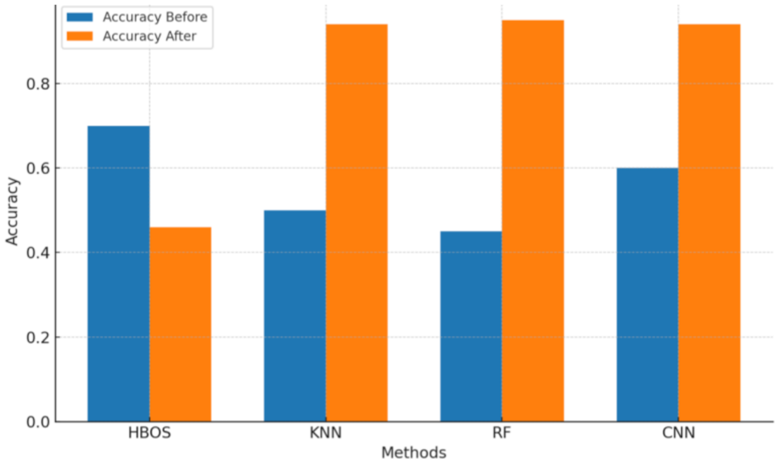


Fig.6. Comparative Performance of Anomaly Detection Algorithms: Impact of Preprocessing Before and After Data Processing

Moreover, these algorithms’ prediction and processing times are comprehensively examined in Fig. 7, which offers a more profound comprehension of their operational dynamics after pre-processing. This comprehensive analysis emphasizes the importance of personalized pre-processing techniques in enhancing the overall performance effectiveness of anomaly detection models in complex and security applications. The Fig. 7, illustrates the performance analysis of a variety of techniques employed in anomaly detection-based access control systems, with an emphasis on their data processing times and prediction capabilities. Four different approaches are evaluated: CNN, KNN, HBOS, and RF. HBOS exhibits low delays for both data processing and prediction, thereby enhancing its overall efficiency. KNN, on the other hand, is distinguished by its significantly high data processing time, which is significantly longer than its prediction time and the overall times of the other methods. This suggests the possibility of a bottleneck. Both CNN and RF (Random Forest) exhibit comparable performance, with relatively low processing and prediction times. CNN, on the other hand, displays slightly higher values than RF. HBOS and RF are more time-efficient, as this analysis emphasizes. However, KNN's extensive processing time may restrict its practical application in time-sensitive applications.

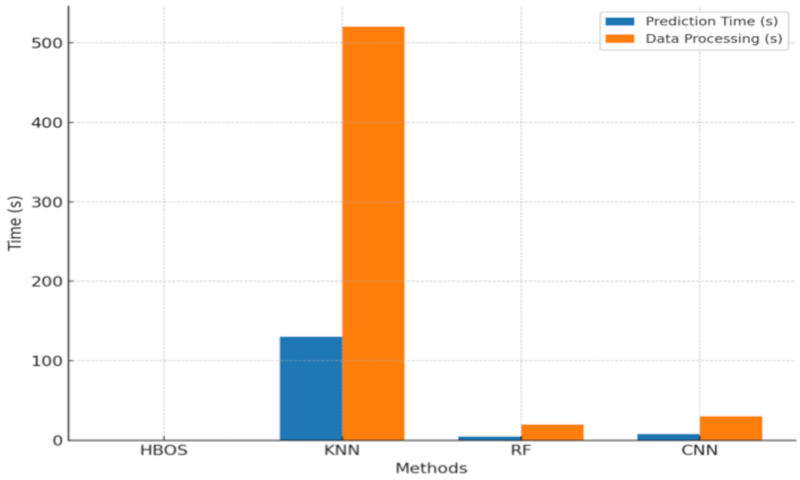


Fig.7. Comparative Analysis of Preprocessing Effects on Real-Time Prediction and Processing Times for Anomaly Detection Algorithms

6.2. Performance Evaluation of Adaptive Policy Adjustment Algorithm

This subsection highlights the analysis of the performance of the adaptive policy adjustment algorithm in access control (APA-AC) across various experimental scenarios, as illustrated in Fig. 8. It determines an optimal threshold that correctly balances the trade-off between false positives (unnecessary access restrictions) and false negatives (unwarranted access permissions). This emphasizes the algorithm's ability to update policies dynamically, improving access control security while preserving untypical users. Additionally, the correlation coefficient shown in the graph quantifies the relationship between each access request pattern and anomalous behavior, demonstrating the algorithm's remarkable ability to change its policies simultaneously. This method can adapt, which may improve the proposed method's reliability and its capacity to prevent threats in various scenarios.

The algorithm effectively enhances security frameworks by adapting real-time access controls according to assessed risks and behavioral analytics. The APA-AC algorithm is designed to adapt to diverse scenarios, ensuring efficient operation irrespective of the complexities associated with access requests or user behaviors. According to Fig. 8, access request features that are strongly associated with abnormal behavior policies are effectively utilized when a threshold value of 0.26 is set. The approach outlined above employs iterative threshold adjustments to guarantee that the access decision-enforcement process only includes features with substantial correlations.

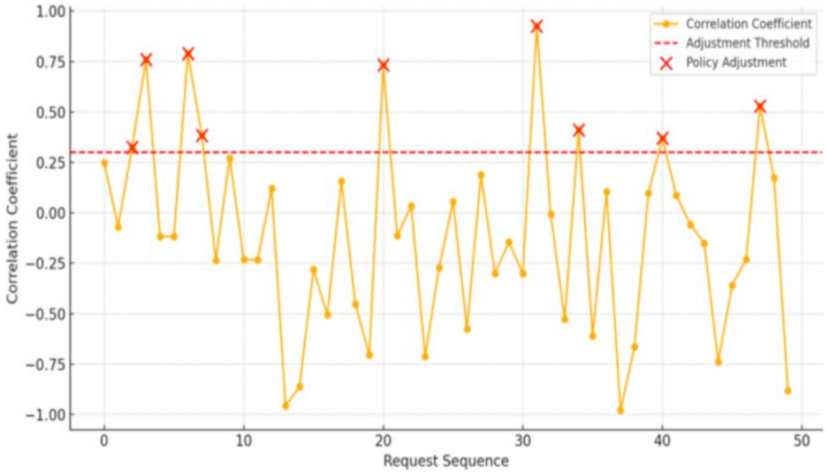


Fig.8. APA Performance Across Risk Scenarios

Lastly, Fig. 9 illustrates the APA-AC algorithm's performance adjustment over time, which is based on dynamic risk attribute evaluations. The stable accuracy criteria demonstrate the algorithm's consistent performance, which effectively balances false positives and negatives to ensure an efficient access control approach. The algorithm's adaptability to changing risk conditions is underscored by the variability in the ROC-AUC metric (dashed orange line), which is achieved by adjusting its decision criteria to maintain high accuracy. This adaptability is essential, allowing the APA-AC algorithm to respond dynamically to new threats and evolving user behaviors. The algorithm has maintained the effectiveness of access control policies and enhanced system security by continuously monitoring and adjusting based on real-time data, resulting in an adaptive adjustment accuracy of 97%.

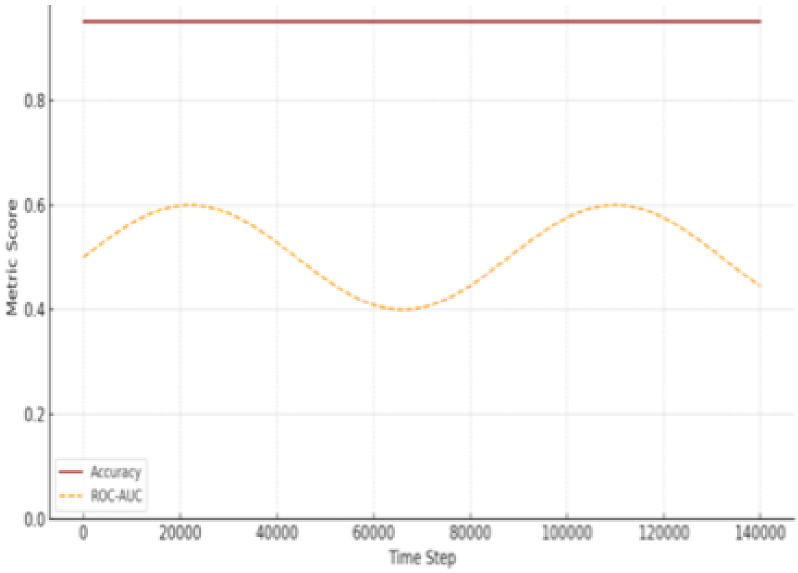


Fig.9. APA Accuracy Adjustment Over Time

7.0. DISCUSSION

As demonstrated by prior research, many access control methods for Bring Your Own Device (BYOD) environments concentrate on a single security layer. As noted in [10], [11], and [12], specific strategies are concentrated on the tactical layer, emphasizing detailed authentication policies. Others emphasize the strategic layer, incorporating risk policies and utilizing machine learning techniques, as exemplified in [16], [18], and [17]. Even though these methods are intended to improve the security of BYOD, they frequently fail due to their reliance on a single layer, selective policy integration, lack of adaptability to the dynamic BYOD environment, and unequal access control and detection mechanisms. Consequently, real-time attack detections frequently necessitate prolonged prediction periods and suboptimal accuracy.

Implementing a multi-layered policy approach is imperative to fortify BYOD access control. In a BYOD context, effective control should encompass three security policy layers: authentication from the tactical layer, risk policy from the strategic layer, and policy management from the operational layer. This approach guarantees robust and efficient security [8]. This study introduces a dynamic access control model that utilizes machine learning to implement an adaptive policy framework for real-time risk monitoring in a BYOD environment. The model incorporates an adaptive policy adjustment algorithm that responds to anomalous access patterns, real-time risk monitoring through anomaly detection, and fine-grained dynamic policy authorization.

In addition, the proposed solution was evaluated and compared to other well-established solutions in the field. The efficacy of our access control system in comparison to existing systems was evaluated in the study, as illustrated in Table 5. Han et al. introduced a risk access control system known as the Intrusion Detection Hyperparameter Control System (IDHCS), which effectively manages and trains a deep neural network (DNN) feature extractor and a k-means clustering module through PPO-based reinforcement learning. The Intrusion Detection and Host-based Collaborative System (IDHCS) effectively manages the Deep Neural Network (DNN) feature extractor to extract the most significant network features, which are then utilized for intrusion detection by applying k-means clustering on the UNSW-NB15 dataset. The system achieves a commendable accuracy rate of 0.94268 [6]. Bhardwaj et al.in [7] proposed a novel risk access control model that integrates a well-defined stacking sparse AutoEncoder (AE) for feature learning with a Deep Neural Network (DNN) for the classification of network traffic into benign or DDoS assault traffic using Naive Bayes. The achieved value was 0.824; this model also applied the support vector machine algorithm and performed with 0.755 accuracy. The previous solution contributed to the network's detection of attacks and monitoring of risks. Nonetheless, these solutions were restricted to a single layer and did not account for the other layers of security policies, so the performance of attack detection accuracy needs improvement.

Table 5. Comparison of Results with Previous Work on UNSWNB15 Dataset

Ref	Method	Performance	Prediction Time(s)	APA
[5], 2023	Hybrid feature selection model (IGRF) limited to strategic layer with suboptimal performance.	84.24%	N/A	N/A
[6], 2022	Deep neural networks and k-means clustering with high accuracy; requires additional security layers.	94.268%	N/A	N/A
[7], 2020	Neural network focused on DDoS traffic classification; limited scope and performance.	82.4%, 75.5%	N/A	N/A
Proposed solution	Comprehensive model with dynamic policies, real-time risk monitoring, and adaptive policy adjustment.	95%	0.5	97%

Consequently, this paper presents an enhanced adaptive policy using machine learning based on real-time risk monitoring within a dynamic access control model. The proposed access control framework effectively addresses security policies' tactical, strategic, and operational layers. The results confirmed that our solution achieved 95% accuracy in attack detection with a prediction time of 0.5 seconds and 97% accuracy in adaptive policy adjustment. The optimal threshold value of 0.26 indicates that the policy adjustment formula effectively employs access request characteristics substantially correlated with the target variable (abnormal behavior policy). In order to address three layers of security policies, this comprehensive approach incorporates access behavior monitoring, adaptive policy adjustment, and dynamic attributes. It satisfies a variety of privacy standards, including authenticity, confidentiality, and the detection of attacks.

Additionally, the solution is context-aware, and it continuously monitors the behavior of access requests to prevent the user from accessing the organization's network and resources. In light of this context, the system adapts its access control policies.

8.0. CONCLUSIONS

Traditional access control systems frequently fail to holistically address security challenges in BYOD environments. This study introduces a tri-layered framework that improves security by implementing adaptive policies that are informed by real-time risk monitoring and dynamic machine learning. The proposed model includes Dynamic Risk Attribute and Anomaly Detection, which utilizes machine learning to promptly identify unusual access requests, and Adaptive Policy Adjustment, which refines policies by analyzing user behavior and recommending updates. The system's high efficacy was demonstrated through validation using the UNSW-NB 15 dataset, which achieved 95% accuracy in anomaly detection within 0.5 seconds and 97% accuracy in policy adjustments with an optimal threshold of 0.26. The model's adaptability to the changing requirements of BYOD security environments is demonstrated by these results, which emphasize its efficacy in administering access control and mitigating insider threats. As a result, this architecture offers a durable solution for improving the security measures of contemporary, dynamic access control systems.

ACKNOWLEDGMENTS. The authors of this paper appreciate the reviewers' observations, comments, and suggestions for improving the manuscript's content. Furthermore, the authors would like to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

REFERENCES

[1] A. V. Herrera, M. Ron, and C. Rabadão, "National cyber-security policies oriented to BYOD (bring your own device): Systematic review," in Proceedings of the 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 21-24 June 2017, pp. 1-4.

[2] B. Tokuyoshi, “The security implications of BYOD,” Network Security, Vol. 2013, No. 4, Apr. 2013, pp. 12-13.

[3] G. Kim, Y. Jeon, and J. Kim, “Secure mobile device management based on domain separation,” in Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, South Korea, 19-21 Oct. 2016, pp. 918-920.

[4] J.-E. Lee, S.-H. Park, and H. Yoon, “Security policy based device management for supporting various mobile OS,” in Proceedings of the Second International Conference on Computing Technology and Information Management (ICCTIM), Johor, Malaysia, 21-23 Apr. 2015, pp. 156-161.

[5] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, “IGRF-RFE: A hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset,” Journal of Big Data, Vol. 10, No. 1, 2023, pp. 1-26.

[6] H. Han, H. Kim, and Y. Kim, “An efficient hyperparameter control method for a network intrusion detection system based on proximal policy optimization,” Symmetry, Vol. 14, No. 1, Jan. 2022, p. 161.

[7] A. Bhardwaj, V. Mangat, and R. Vig, “Hyperband tuned deep neural network with well-posed stacked sparse autoencoder for detection of DDoS attacks in cloud,” IEEE Access, Vol. 8, 2020, pp. 181916-181929.

[8] A. G. Bello, D. Murray, and J. Armarego, “A systematic approach to investigating how information security and privacy can be achieved in BYOD environments,” Information & Computer Security, 2017.

[9] K. Yanson, “Results of implementing WPA2-enterprise in educational institution,” in Proceedings of the IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 12-14 Oct. 2016, pp. 1-4.

[10] V. Gkamas, M. Paraskevas, and E. Varvarigos, “Design of a secure BYOD policy for the Greek school network: A case study,” in Proceedings of the IEEE Intl Conference on Computational Science and Engineering (CSE), Paris, France, 24-26 Aug. 2016, pp. 557-560.

[11] O. Oluwatimi, M. L. Damiani, and E. Bertino, “A context-aware system to secure enterprise content: Incorporating reliability specifiers,” Computers & Security, Vol. 77, 2018, pp. 162-178.

[12] B. L. D. Seneviratne and S. A. Senaratne, “Integrated corporate network service architecture for bring your own device (BYOD) policy,” in Proceedings of the 3rd International Conference on Information Technology Research (ICITR), Moratuwa, Sri Lanka, 5-7 Dec. 2018, pp. 1-6.

[13] D. Kim and S. Lee, “Study of identifying and managing the potential evidence for effective Android forensics,” Forensic Science International: Digital Investigation, Vol. 33, 2020, p. 200897.

[14] [14] A. Aldini, J.-M. Seigneur, C. Ballester Lafuente, X. Titi, and J. Guislain, “Design and validation of a trust-based opportunity-enabled risk management system,” Information & Computer Security, 2017.

[15] M. Ammar, M. Rizk, A. Abdel-Hamid, and A. K. Aboul-Seoud, “A framework for security enhancement in SDN-based datacenters,” in Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 21-23 Nov. 2016, pp. 1-4.

[16] M. I. Ali, S. Kaur, A. Khamparia, D. Gupta, S. Kumar, A. Khanna, and F. Al-Turjman, “Security challenges and cyber forensic ecosystem in IoT driven BYOD environment,” IEEE Access, Vol. 8, 2020, pp. 172770-172782.

[17] D. Petrov and T. Znati, “Context-aware deep learning-driven framework for mitigation of security risks in BYOD-enabled environments,” in Proceedings of the 4th IEEE International Conference on Collaboration and Internet Computing (CIC), Philadelphia, PA, USA, 18-20 Oct. 2018, pp. 166-175.

[18] A. M. Alghamdi and K. Almarhabi, “A proposed framework for the automated authorization testing of mobile applications,” International Journal of Computer Science & Network Security, Vol. 21, No. 5, 2021, pp. 217-221.

[19] C. Xiang et al., “Towards continuous access control validation and forensics,” in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11-15 Nov. 2019, pp. 113-129.

[20] L. Argento et al., “Towards adaptive access control,” in Proceedings of Data and Applications Security and Privacy XXXII: 32nd Annual IFIP WG 11.3 Conference, DBSec 2018, Bergamo, Italy, 16-18 July 2018, pp. 99-109.

[21] A. Alkhresheh, K. Elgazzar, and H. S. Hassanein, “Adaptive access control policies for IoT deployments,” in Proceedings of the International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15-19 June 2020, pp. 377-383.

[22] V. Gumma, B. Mitra, S. Dey, P. S. Patel, S. Suman, and S. Das, “PAMMELA: Policy administration methodology using machine learning,” arXiv preprint, arXiv:2111.07060, 2021.

[23] [23] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, “A role-based access control model and reference implementation within a corporate intranet,” ACM Transactions on Information and System Security (TISSEC), Vol. 2, No. 1, 1999, pp. 34-64.

[24] T. Cover and P. Hart, “Nearest neighbor pattern classification,” IEEE Transactions on Information Theory, Vol. 13, No. 1, 1967, pp. 21-27.

[25] I. Aguilera-Martos et al., “Multi-step histogram based outlier scores for unsupervised anomaly detection: ArcelorMittal engineering dataset case of study,” Neurocomputing, Vol. 2023, p. 126228.

[26] V. C. Hu, D. Ferraiolo, R. Kuhn, and A. R. Friedman, Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft), NIST Special Publication, 800-162, 2013.

[27] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in Proceedings of the Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10-12 Nov. 2015, pp. 1-6.