Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.055287

ARTICLE

Adaptable and Dynamic Access Control Decision-Enforcement Approach Based on Multilayer Hybrid Deep Learning Techniques in BYOD Environment

Aljuaid Turkea Ayedh M[1,2,*], Ainuddin Wahid Abdul Wahab[1,*] and Mohd Yamani Idna Idris[1,3]

[1]Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

[2]Faculty of Computer Science and Information Technology, Shaqra University, Shaqra, 11961, Saudi Arabia

[3]Center for Mobile Cloud Computing, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

*Corresponding Authors: Aljuaid Turkea Ayedh M. Email: taljuaid@su.edu.sa; Ainuddin Wahid Abdul Wahab. Email: ainuddin@um.edu.my

Received: 22 June 2024 Accepted: 13 August 2024 Published: 12 September 2024

ABSTRACT

Organizations are adopting the Bring Your Own Device (BYOD) concept to enhance productivity and reduce expenses. However, this trend introduces security challenges, such as unauthorized access. Traditional access control systems, such as Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC), are limited in their ability to enforce access decisions due to the variability and dynamism of attributes related to users and resources. This paper proposes a method for enforcing access decisions that is adaptable and dynamic, based on multilayer hybrid deep learning techniques, particularly the Tabular Deep Neural Network TabularDNN method. This technique transforms all input attributes in an access request into a binary classification (allow or deny) using multiple layers, ensuring accurate and efficient access decision-making. The proposed solution was evaluated using the Kaggle Amazon access control policy dataset and demonstrated its effectiveness by achieving a 94% accuracy rate. Additionally, the proposed solution enhances the implementation of access decisions based on a variety of resource and user attributes while ensuring privacy through indirect communication with the Policy Administration Point (PAP). This solution significantly improves the flexibility of access control systems, making them more dynamic and adaptable to the evolving needs of modern organizations. Furthermore, it offers a scalable approach to manage the complexities associated with the BYOD environment, providing a robust framework for secure and efficient access management.

KEYWORDS

BYOD; security; access control; access control decision-enforcement; deep learning; neural network techniques; TabularDNN; multilayer; dynamic; adaptable; flexibility; bottlenecks performance; policy conflict

1 Introduction

The widespread adoption of Bring Your Own Device (BYOD) in workplaces has become increasingly prevalent as employees bring their personal devices, such as smartphones, smartwatches, laptops, and tablets. This trend has resulted in significant business advantages, including reduced

organizational costs and improved productivity when employees use their devices. Implementing BYOD policies and access control technology is crucial for regulating and securing this practice [1]. These policies define restrictions and permissions to prevent unauthorized users from accessing the corporate network and its resources, aiming to ensure the security and privacy of users and their data within the organization [2].

The successful implementation of BYOD policies and access control solutions is critical for organizations but faces numerous challenges, with security being a primary concern. The dynamic nature of BYOD access control systems and the need for consistent policies present a formidable obstacle. In a university setting, for instance, a diverse array of devices across multiple departments and campuses, along with numerous entities accessing servers simultaneously, exemplifies this complexity. Existing access control policies often limit the flexibility that BYOD requires, relying on specific attributes and limited entities, resulting in a rigid framework that struggles to adapt to minor user and resource variable variations. Access decision enforcement in traditional access control systems, including role-based access control (RBAC), attribute-based access control (ABAC), or relationship-based access control (RBAC), often faces limitations due to the dynamic nature of the BYOD environment [3]. Minor changes in user and resource properties can significantly impact access control status, leading to challenges for system administrators. These challenges necessitate constructing complex rules with numerous conditions and permissions for decision control. Consequently, traditional systems encounter policy conflicts, decision-making bottlenecks, delayed access response times, and mediocre performance.

Several methodologies have been suggested to tackle these difficulties. Cappelletti et al. [4] employed historical access logs to augment decision-making processes; however, the time required for analyzing log features could have a detrimental effect on performance. Khilar et al. [5] introduced a trust-based mechanism that utilizes machine learning to achieve 92.1% accuracy in making access decisions. This mechanism takes into account user behavior and authorization history. However, the reliance on user attributes in access requests constrains this method, potentially causing delays in decision implementation and creating performance obstacles.

Moreover, in a study conducted by Srivastava et al. [6], a Risk Access Control (RAAC) system using the random forest algorithm was implemented to improve decision-making accuracy. The system achieved an accuracy rate of 93.33%. Despite the effectiveness of the system, operational efficiency is hindered by challenges such as decision time and feature engineering. You et al. [7] introduced the Boosting Window (BW) algorithm to create an access control knowledge graph, achieving a decision-making accuracy of 89.64.

This paper presents an advanced, flexible method for enforcing access decisions using a multilayer hybrid deep learning approach. The objective is to reduce performance limitations in access decision-making, resolve delays in decision time caused by complex policy engineering, and overcome restrictions in decision-making based on inflexible rules or specific attributes. The essence of this methodology is based on neural network algorithms, which carefully analyze the attributes of access requests, including the attributes of the user (Subject) and the resource (Object) across multiple layers. These algorithms condense the input data into binary results, granting or denying access. This approach facilitates the efficient resolution and authorization of access requests by utilizing various user and source attributes. It is not restricted to specific features or policies, allowing it to maintain adaptability and dynamism while addressing inflexibility. Consequently, it substantially decreases time expenditures by eliminating the reliance on the access decision in the policy engineering process. Additionally, it enhances security, distributes access control, and mitigates organizational and administrative difficulties.

The main component of this approach is based on TabularDNN, which effectively handles access requests by analyzing metadata containing user and resource attributes. The TabularDNN model analyzes access patterns and decision rules in different layers, allowing for accurate determinations and immediate adjustments for dynamic access decisions. This comprehensive strategy guarantees the ability to adjust to changing access patterns and security requirements, effectively meeting users' changing needs and the evolving threat landscape.

The suggested approach utilizes various levels of traditional and hybrid deep learning algorithms. Of all the options, the Tabular Deep Neural Network (TabularDNN) is the best choice in our strategy. It has the highest accuracy and effectiveness when implementing access control decisions. The proposed solution is implemented by balancing the data set, developing training and test models, and implementing access decision mechanisms. All of these steps are included in the implementation process. We conducted multiple experiments and utilized the Kaggle Amazon access control policy dataset to assess the effectiveness of the suggested solution. We evaluate performance metrics by comparing the efficiency of different deep learning algorithms and assessing their accuracy in relation to previous methodologies. The results indicate a 94% accuracy in implementing the access decision. The solution streamlines administrative processes while simultaneously improving the adaptability and flexibility of the implementation of access decisions. Following are some of the key contributions of this research:

- Examine and assess the existing approaches for enforcing access decisions in access control systems, considering both conventional methods and machine learning techniques. Identify the drawbacks of these methods, such as conflicts in policies, difficulties in scaling, performance limitations, and decreasing accuracy over time due to growing complexity and dynamism.
- Present an innovative permission decision engine that employs deep learning neural networks to address the determined constraints. This engine classifies permission requests into binary categories using various levels of analysis. Additionally, it employs hybrid technology to simplify the enforcement of access permissions, regardless of whether they are granted or denied.
- Enhance the current access control system by transforming the Policy Decision Point (the component responsible for enforcing access decisions) to be flexible and responsive using deep learning technology, rather than relying on predetermined rules and rigid architecture.
- Improve the accuracy of enforcing access decisions in security control systems by balancing datasets and performing experiments to identify the most effective strategies, thereby improving the dependability and efficacy of the suggested solution.
- Employ several types of deep learning models, such as Multi-Layer Perceptron (MLP) and hybrid models that integrate different architectures, including LSTM-GRU Hybrid, Conv1D-GRU Hybrid, Conv1D-RNN Hybrid, Multi-Channel Conv1D (MConv1D), RNN-dense, and Tabular DNN Models. This investigation enhances the understanding of the performance of various architectures in enforcing access decisions.
- Evaluate the proposed solution using the Amazon Access Control Policy dataset to demonstrate its effectiveness and resilience. Include an array of metrics, such as the F1 score, AUC (Area Under the Curve) score, training loss, and validation loss, alongside precision, recall, and accuracy, to comprehensively assess the model's performance.
- Compare the suggested method against traditional deep learning approaches and other hybrid models, and assess its performance relative to existing techniques.
- Protect policy information during permission decisions with an independent policy decision point, isolating access decision enforcement from policy administration. This results in a secure, efficient, and lightweight access control method.

The remaining sections of this paper are organized as follows: Section 2 provides a comprehensive review of relevant studies on access control and decision-making techniques. Section 3 introduces the proposed model and elaborates on the detailed implementation steps. Section 4 details the implementation process and outlines the evaluation metrics. Section 5 presents an analysis of the results. Subsequently, Section 6 discusses and compares the results with previous work. Finally, Section 7 presents the conclusion of the paper.

2 Related Work

The pertinent literature can be categorized into two main sections. Initially, emphasis is placed on implementing access decision enforcement grounded in roles, addressing a research challenge within conventional access control systems, such as their rigidity and static nature. When expanding the scope of policies, the execution of access control decisions could be improved, leading to role proliferation and policy conflicts, ultimately causing elevated maintenance expenses. The second segment delves into the application of machine learning for enforcing access decisions, highlighting how the integration of machine learning techniques in access control decision-making has mitigated issues associated with traditional access control methods. However, existing machine learning-based access decision enforcement methods have limitations, including performance bottlenecks that result in suboptimal policy decision point performance and substantial time costs.

2.1 Traditional Approach Based Access Decision Enforcement

This section summarizes relevant research focusing on strategies for enforcing access decisions. Existing access control systems often rely on static roles and rigid constraints, limiting flexible access capabilities for Bring Your Own Device (BYOD) users. Lee et al. [8] proposed an access control system utilizing Mobile Device Management (MDM), where access decisions are based on predefined static policies set by administrators. However, this approach lacks adaptability, increasing maintenance costs for unforeseen access requests in the context of BYOD-enabled educational networks, Yanson [9] observed using WPA2-enterprise authentication and predetermined rules for access decision implementation. Similarly, Gkamas et al. [10] introduced a secure access control policy for the Greek Schools Network, outlining access to network resources. A common theme in these approaches is the reliance on static considerations, such as identity verification, for access decision-making. Oluwatimi et al. [11] proposed a proximity-based access control system using accelerometers and fingerprint sensors, employing biometrics to evaluate users' behavioral and physiological characteristics for access determination. Seneviratne et al. [12] implemented an access control solution integrated with existing authentication systems, managing BYOD access through predefined policies for individual users or groups.

2.2 Machine Learning Approach Based Access Decision Enforcement

The positive impact of machine learning on access control has been established, demonstrating significant potential for further development. Machine learning is increasingly utilized for security purposes, with its application extending to various contexts such as policy decision-making, verification and testing, administration, monitoring, and policy extraction. This study focuses on the role of machine learning in access decision-making, its impact on system performance, and its effectiveness in addressing challenges within the traditional Policy Decision Point (PDP) of access control.

Chang et al. [13] introduced a method for time-limited access control that uses Support Vector Machines (SVMs) to train machine learning models. These models leverage both user and resource

information to determine whether to grant or deny access requests. Additionally, they can predict future access decisions by analyzing metadata and characteristics related to users and resources. While effective, this approach requires significant feature engineering and bases its decision-making on the temporal aspects of access requests. This solution can lead to performance bottlenecks in the access decision unit, especially when processing high requests, a common scenario for large and complex organizations.

Cappelletti et al. [4] introduced an innovative access control methodology to improve decision-making processes by leveraging historical database access logs. The essence of their approach is employing machine learning models, which are meticulously trained on these logs. This strategy is particularly beneficial in dynamic settings where data undergoes frequent updates and is accessed by diverse users. However, the approach necessitates significant time for analyzing the features within the access logs and making informed access decisions. This requirement may lead to adverse effects on performance, especially at critical policy decision points, such as bottlenecks in performance, thereby impacting the overall efficiency of access control decision-making processes.

Furthermore, Khilar et al. [5] presented a trust-based mechanism leveraging machine learning to grant access to cloud resources. This method considers user behavior and authorization history, employing the random forest and k-NN (k-nearest neighbors) algorithms. It achieved an accuracy of 92.1% in access decision-making. Despite its advantages, this approach has inherent limitations. The effectiveness of decisions heavily relies on the user attributes in the access request, potentially extending the time required to implement decisions and leading to potential performance bottlenecks in the access decision-making process. In addition, Srivastava et al. [6] developed a machine learning-based Risk Access Control (RAAC) system for making access decisions. This system employs the random forest algorithm, factoring in variables such as access time, location, frequency of requests, and resource sensitivity. This method demonstrated high effectiveness, achieving a decision-making accuracy of 93.33%. However, the extensive time required for feature engineering within the access request process emerged as a critical bottleneck, impacting the system's operational efficiency. Future enhancements could focus on streamlining the feature engineering phase or exploring alternative algorithms to mitigate this limitation, thereby improving the access decision-making system's performance and applicability in real-time environments.

Moreover, You et al. [7] proposed a decision-making-based Boosting Window (BW) algorithm to construct an access control knowledge graph. It achieved a performance accuracy of 89.64%, although there remains a need to improve the performance of access decision-making further. Conversely, Karimi et al. [14] introduced an adaptive decision-making framework based on reinforcement learning algorithms, yet encountered challenges in policy decision point performance and overlooked the access response time. Finally, study [15] presented a machine learning method based on a random forest algorithm to enhance access control's policy decision points (PDPs) by using binary classification to grant or deny access. It introduces a vector decision classifier to create dynamic, distributed PDPs that manage security policies with high privacy, thus improving the security and adaptability of the access control system.

Despite advancements through machine learning, issues such as Policy Decision Point (PDP) bottlenecks, delays in decision times, and challenges in addressing unexpected access requests persist. This paper proposes a novel approach to enhance dynamic access control decision-making by integrating deep learning technology. Our solution addresses these challenges by utilizing a decision implementation unit that processes the attributes of access requests covering the requester, the resource, the process, and the authentication policies through deep learning's multi-layered analysis. This

method ensures high performance and low time costs by accurately determining access decisions. In situations where there is a conflict between performance and accuracy or when facing bottlenecks, our approach simplifies the decision to a binary outcome: granting or denying access. This streamlined decision-making process ensures efficiency and reliability in dynamic access control, significantly improving existing methods.

2.3 Policy Mining Approach Based Access Decision Enforcement

Policy mining techniques are crucial for influencing enforcement decisions in security access control systems. They play a vital role in efficiently managing access control policies, determining user permissions to various resources within an information system. Typically, policy mining techniques use user/resource attributes and the system's current access control state as inputs. For Attribute-Based Access Control (ABAC) and Relationship-Based Access Control (ReBAC), these algorithms produce a set of rules (policies) that grant specific permissions. Conversely, Role-Based Access Control (RBAC) mining algorithms output permissions to roles (PA) and user to roles (UA) assignments.

In [16], researchers introduced the Decision Tree ReBAC Miner (DTRM), an innovative algorithm capable of generating policies across various ReBAC languages. This algorithm utilizes decision tree methodologies to extract policies in the latest version of the Object-oriented Relationship-based Access-control Language (ORAL), which now includes two additional set comparison operators, enhancing its predecessor's capabilities. The approach involves training decision trees to classify feature vectors accurately. These vectors are associated with Boolean values that indicate whether a user is authorized to interact with certain resources. inaddtional, The authors of [17] presented an efficient and scalable ReBAC policy mining algorithm. They chose a neural network for its superior handling of high-dimensional data and large datasets, setting it apart from other classification methods for feature selection. This algorithm assigns Boolean values to various feature vectors, indicating whether a user is authorized to perform an action on resources. Each feature in the vector represents either a subject or a resource atomic condition.

Karimi et al. [18] introduced a method for automating the extraction of ABAC policies using an unsupervised learning approach to mine ABAC policies from access logs. This method can derive policy rules that include both positive and negative attributes, as well as relationship-based filters. morever, In [19], Jabal et al. proposed a novel framework for learning ABAC policies named Polisma, combining data mining, statistical, and machine learning techniques. The Polisma approach consists of four main stages. It applies Random Forest (RF) and K-Nearest Neighbors (KNN) as machine learning classifiers on requests not covered by the policies learned in the first three stages, using the classification results to label these data and generate additional rules. The approach is evaluated empirically using both real-world and synthetic datasets. Experimental results show that Polisma can develop ABAC policies that accurately control access requests.

3 Proposed Model

The proposed solution introduces an access decision enforcement approach, utilizing deep learning techniques. In contrast, conventional access control models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), rely on fixed rules or user/resource attributes to make access decisions., where access decisions are typically based on predetermined rules or specific attributes. Moreover, some existing access models employ machine learning to make access decisions. It provides more flexibility and dynamic but often requires time to engineer attributes or policies to make access decisions. It may lead to potential inefficiencies and delays in access decision

enforcement and cause performance bottlenecks. This model implements access decisions by utilizing deep learning algorithms that make access decisions based on many inputs related to user resource and role authorization and process through layered to get a permit or deny. It will provide more adaptable and accurate access decisions.

In contrast, the proposed solution harnesses the power of deep learning techniques to efficiently handle access decisions by considering a broader range of elements, including user attributes, resource attributes, and authorization policies. This approach enables the model to adapt more seamlessly to diverse regulatory environments and dynamic access control requirements. Moreover, its broad descriptiveness facilitates context-sensitive decision-making, enhancing flexibility and adaptability.

By leveraging deep learning, the proposed solution effectively addresses critical challenges in traditional access control systems, such as inflexibility, policy conflicts, and performance bottlenecks. Deep learning's ability to learn from data allows for more dynamic and agile control frameworks for access management. This departure from conventional methods underscores the fundamental disparity between the proposed model and previous solutions, highlighting its potential to revolutionize access control practices and address the evolving needs of modern organizations.

3.1 Comparison of Traditional Access Decision Enforcement in Access Control vs. the Proposed Solution

The main points in this section highlight the differences between the suggested solution and alternative approaches. Specifically, it contrasts the use of deep learning methodologies for access decision-making with traditional machine learning techniques, as depicted in Fig. 1. Furthermore, Table 1 elucidates the primary differences between the existing approaches and the proposed solution. Subsequently, the following points will elaborate on the methodology employed to investigate policies that inform access decision-making, and they will also delineate the implementation process for handling access requests to enforce access decisions.

- **Based on Policy Mining Technique:** Policy mining techniques are utilized in current access decision enforcement solutions to govern access decisions, as depicted in Fig. 1. This approach involves receiving an authorization policy and utilizing resource metadata as inputs. Subsequent policy engineering is required concerning the type of access control—be it attribute-based access control (ABAC) or role-based access control (RBAC). The outputs are either user assignments and permission assignments for RBAC or access control rules for ABAC. However, this does not constitute the final step in access decision enforcement; it necessitates the integration of an additional model to implement access decisions based on the outputs from the initial stage. This highlights the limitations of this technique in access decision enforcement and underscores the time required to assess all processes naturally impacted by security access control within the environment.
- **Based on Traditional Machine Learning Techniques:** As illustrated in Fig. 1, this approach initiates by receiving an access request, along with the authorization policy, and metadata concerning users and resources as inputs. The procedure then involves further feature or policy engineering based on specific attributes or policy requirements. The outcome of this method is the access decision. This technique offers increased flexibility and enhances the enforcement of access decisions. However, it exhibits limitations in adaptability, particularly regarding the specific attributes or rules needed to enforce decision-making, which are critical in complex environments. Moreover, the time required for additional engineering of attributes to ensure accurate access decisions adversely impacts the response time for access requests.

- **Based on the Proposed Solution:** As depicted in Fig. 1, the proposed solution employs a multi-layer neural network deep learning technique to streamline access control by eliminating the need for feature engineering. It directly uses metadata from user and resource access requests. The solution centers on a deep neural network that processes this metadata to make swift access control decisions, marking a paradigm shift from traditional methods. This approach inputs inherent metadata like access logs, employee join dates, and network profiles. Unlike traditionally engineered attributes, this metadata is part of the system's functionalities and is available immediately post-implementation, facilitating prompt and adaptive decision-making. For instance, in diverse organizational settings with applications such as email and file storage, each contributes specific metadata like 'join date' and 'spending history.' This metadata, integral to the system rather than crafted during the design phase, provides a comprehensive, real-time view of the user and resource contexts, ensuring a responsive access control mechanism apt for modern organizational complexities.

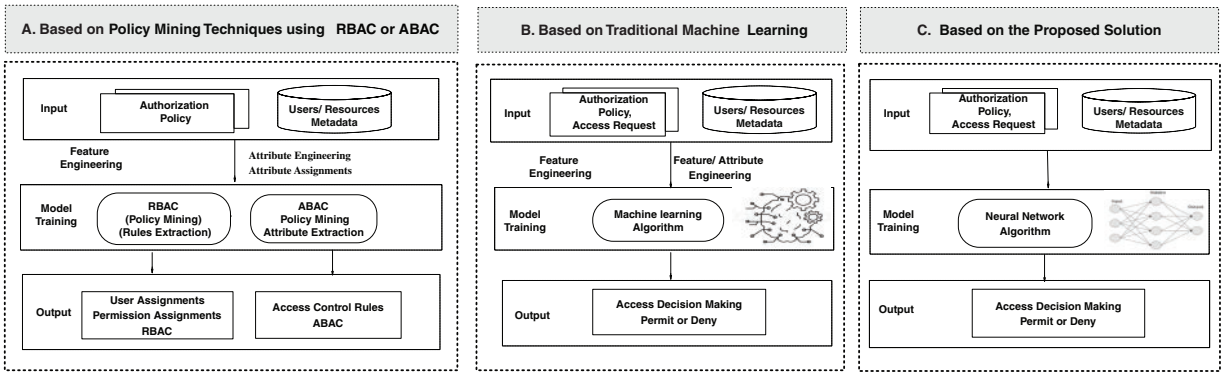

Figure 1: Comparison of existing access decision enforcement *vs.* the proposed solution

Table 1: Comparison of existing access decision enforcement *vs.* the proposed solution

Criteria	Policy mining technique	Traditional machine learning	Proposed solution
Input	Authorization policy, attributes	Authorization policy, attributes	User/resource metadata, Authorization policy
Feature/policy engineering	Required	Required	No required; Processes metadata from current access request
Access decision enforcement (Output)	No, Permission assignments or Rules	Yes	Yes
Access decision time	Slow	Slow	Fast
Adaptability	Limited	Limited, based on specific attributes or roles.	High

3.2 Adaptable and Dynamic Access Control Decision-Enforcement Approach Based on Multilayer Hybrid Deep Learning Techniques

The proposed solution, an adaptive and dynamic access control decision-making leveraging multi-layer hybrid deep learning techniques, signifies a significant advancement in access control systems. By incorporating deep learning methodologies into the access decision-enforcement framework, the system showcases its capacity to adapt and react dynamically. It eschews reliance on predetermined rules or features for decision-making, opting to analyze user, resource, and operation data. Utilizing multi-layer hybrid deep learning techniques facilitates intricate analysis of access requests across various layers, thereby ensuring the precision of authorization decisions. Fig. 2 elucidates the overarching structure of the enhanced access decision-making model for access control utilizing deep learning methodologies.

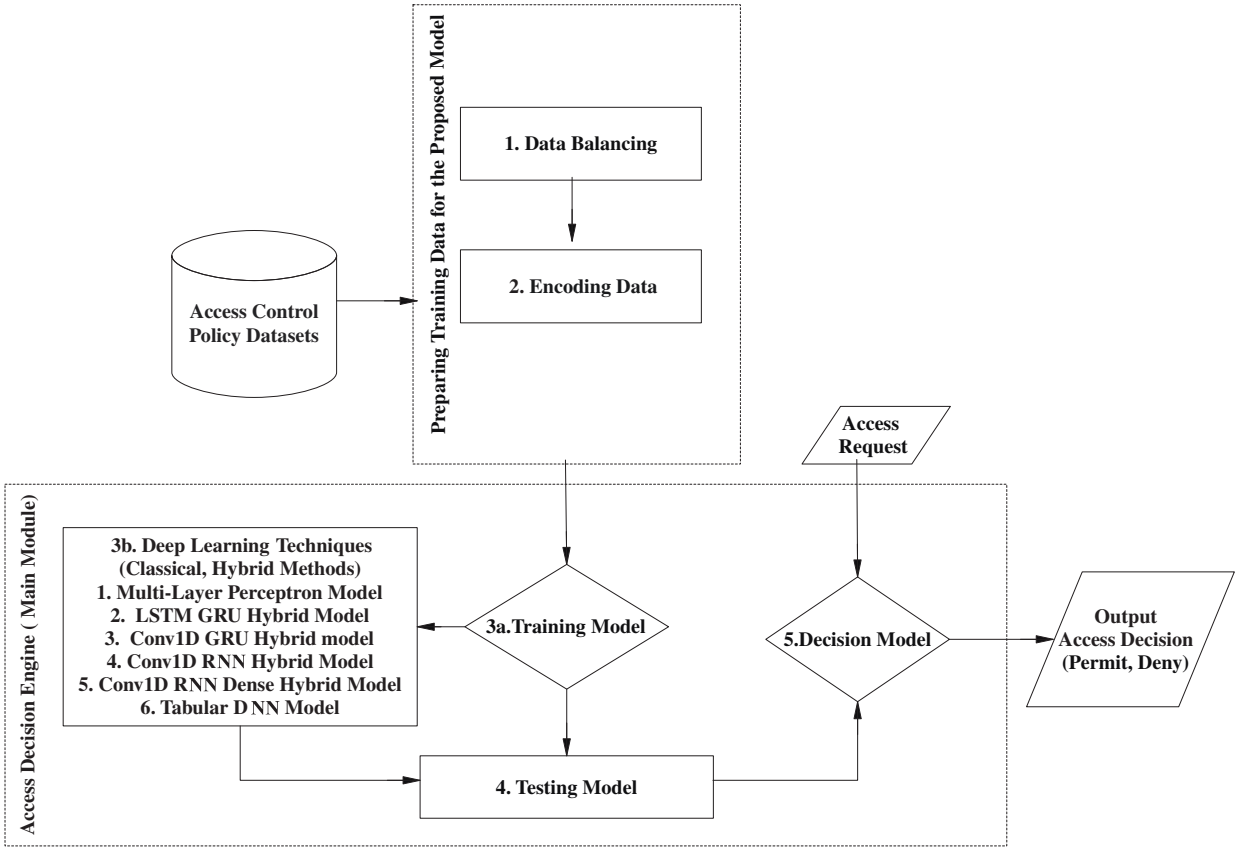

Figure 2: Adaptable and dynamic access control decision-enforcement approach based on deep learning techniques

The proposed solution employs classical neural networks, including Multi-Layer Perceptrons (MLPs), as well as hybrid methods utilizing multiple layers such as Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and various hybrid architectures. Specifically, these architectures include:

- **MLP Technique:** This model comprises numerous layers, including an input layer, hidden layers, and an output layer. A more robust decision-making system is facilitated by the connection of each node in one layer to every node in the subsequent layer.
- **LSTM GRU Hybrid Technique:** The Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) architectures are combined in a synergistic manner to effectively leverage their respective advantages in the modeling of sequences and the capture of temporal dependencies.
- **Conv1D GRU Hybrid Technique:** Combining the spatial feature extraction of Conv1Ds with the temporal information processing capability of GRUs, the novel Conv1D GRU Hybrid enables more sophisticated and efficient data analysis.
- **Conv1D RNN Hybrid Technique:** It incorporates Dense layers into Conv1D RNNs, providing full connectivity between every input through spatial arrangement before processing them further according to their order.
- **Conv1D RNN Dense Hybrid Technique:** It enhances Conv1D RNNs with Dense layers, allowing for complete connectivity between all inputs via spatial arrangement, and then processes them in the order they were received.
- **Tabular DNN Technique:** This method is specifically tailored to handle arranged information by utilizing fully interconnected layers, called Dense layers, to capture and analyze relationships and patterns in tabular data.

This comprehensive architecture encompasses several stages: the data balancing model, the feature processing model, the training model, the testing model, and the access decision enforcement model.

- **Balancing Datasets:** We utilize the Amazon Kaggle dataset, a publicly accessible repository hosted on Kaggle. This dataset is a comprehensive archive of access control decisions, with data about approximately 9000 users and 7000 resources, totaling over 32,000 authorization records. Each entry includes eight user characteristics, a resource identifier, and a binary action label indicating access requests' approval (1) or rejection (0). A primary challenge in this dataset is the imbalance in class labels, where the 'deny permission' category (y = 0) significantly outweighs the 'grant permission' category (y = 1), initially presenting counts of ($y = 0{:}30,872$ and $y = 1{:}1897$). This imbalance can impair the model's ability to effectively learn from the less represented class, potentially diminishing predictive accuracy. To address this issue, we implement a strategy that involves modifying the weights assigned to each category. We adopt a strategy that adjusts the weights assigned to each category, executed through a series of defined steps.
  - Define the initial class distribution in a dataset with binary classification. Let n_0 and n_1 be the number of instances for Class 0 and Class 1, respectively.
  - The weight w_i for Class i can be calculated as:

$$w_i = \frac{N}{2 \times n_i} \tag{1}$$

    where N is the total number of samples, $N = n_0 + n_1$.
  - The loss function L, adjusted for class weights, is given by:

$$L = \sum_{i=1}^{N} w_{y_i} \cdot \ell(f(x_i), y_i) \tag{2}$$

    y_i is the class label, $f(x_i)$ is the model prediction for sample x_i, ℓ is the loss incurred (e.g., cross-entropy), and w_{y_i} is the weight for the class y_i.

- **Encoding Data:** In the proposed deep learning model for encoding an access control policy dataset, each access request P_i is represented as a vector $\mathbf{v}_i$. The encoding process transforms the access request attributes into a high-dimensional space using a neural network. The encoding function f applied to access request P_i can be represented by the following equation:

$$\mathbf{v}_i = f(\mathbf{x}_i; \theta) \tag{3}$$

where $\mathbf{x}_i$ denotes the input features of policy P_i, and θ represents the parameters of the neural network model.

- **Training Model:** The study employs various deep learning models, including the Multi-Layer Perceptron (MLP) and hybrid models that integrate diverse architectures such as the LSTM-GRU Hybrid, Conv1D-GRU Hybrid, Conv1D-RNN Hybrid, Multi-Channel Conv1D (MConv1D), RNN-Dense, and Tabular DNN Models. Additionally, the research integrates classical approaches and advanced hybrid methods across multiple layers to enhance access decision enforcement. This comprehensive exploration aids in understanding the performance of different architectures in managing access control.

  The proposed Tabular DNN architecture capitalizes on metadata associated with users and resources as inputs. It features a classification layer where each neuron is designated to compute the likelihood of authorizing a specific action, denoted as "op." The decision-making process involves comparing the permission probability, derived from the output neuron, against a preset threshold. Formally, given a feature vector x representing user and resource metadata, the architecture functions as a predictive model f, yielding an outcome $\hat{y} = f(x)$ which indicates whether to permit (1) or refuse (0) the operation op.

  The training optimization utilizes a dataset X consisting of N authorization tuples (x_i, y_i), where x_i includes the metadata and y_i signifies the desired outcome op. The core functionality of this Tabular DNN model in the context of access decision enforcement is encapsulated by the following equation:

$$\text{output} = \sigma\left(W_n \cdot \text{ReLU}\left(\ldots \text{ReLU}\left(W_2 \cdot \text{ReLU}\left(W_1 \cdot x + b_1\right) + b_2\right) \ldots + b_{n-1}\right) + b_n\right) \tag{4}$$

  where
  - x represents the input vector containing features relevant to the access decision.
  - W_i and b_i denote the weights and biases of the i-th layer, respectively.
  - ReLU is employed as the activation function in hidden layers to introduce non-linearity.
  - σ is the sigmoid activation function in the output layer, generating a probability output between 0 and 1, indicating the likelihood of access approval.

- **Testing Model:** In order to evaluate and validate the performance of the trained models, a distinct test set was extracted from the dataset while preserving the proportionality of class labels consistent with the training data. This test set remained consistently employed for evaluating the models' performance across all experimentation phases. This methodological approach guarantees an equitable and impartial assessment of the models on unseen data, thereby facilitating insights into their generalization capabilities. The following is the fundamental equation that describes model testing:

$$\hat{y}\text{new} = \sigma(\mathbf{w}^\top \mathbf{x} + b) \tag{5}$$

  where $\hat{y}$ is the predicted probability of granting access, σ is the sigmoid function, $\mathbf{w}$ is the weight vector, $\mathbf{x}$ is the input feature vector, and b is the bias.

- **Access Decision Enforcement:** In the proposed framework, the access control decision engine plays a crucial role in managing and sanctioning access requests. This engine leverages deep

learning technology and utilizes three primary inputs: the user, the resource, and the desired operation. The process begins with the engine examining metadata related to both the user and the resource. This metadata is then encoded into a binary format suitable for analysis by a neural network. Mathematically, let U represent the user, R the resource, and O the desired operation. The metadata for U and R is encoded into binary vectors $\mathbf{u}$ and $\mathbf{r}$, respectively. These vectors are concatenated to form a single input vector $\mathbf{x}$ where $\mathbf{o}$ is the binary representation of O:

$$\mathbf{x} = [\mathbf{u}, \mathbf{r}, \mathbf{o}] \tag{6}$$

The neural network function $f(\mathbf{x})$ processes the input vector to produce an output y, which determines the access decision:

$$y = f(\mathbf{x}) \tag{7}$$

If $y \geq \theta$, where θ is a predefined threshold, the access request is granted; otherwise, it is denied. Thus, the decision rule can be formulated as:

$$\text{Decision} = \begin{cases} \text{Grant access} & \text{if } y \geq \theta \\ \text{Deny access} & \text{if } y < \theta \end{cases} \tag{8}$$

Permissions are allocated across various processes, allowing the decision engine to dynamically revoke access rights based on the initial request and network predictions. For instance, consider the following scenario: Alice, a user, requests access to the resource "projectA." If the desired operation 'op2' is executed, the decision engine will grant authorization to Alice at this access level, provided the neural network produces a positive output (i.e., $y = 1$) for 'op2'.

4 Implementation and Model Evaluation

This section discusses the experiment's tools,datasets and performance metrics.

4.1 Datasets and Tools

In our study, we utilize the Amazon Kaggle dataset, a publicly available resource on Kaggle, to evaluate security access control mechanisms. This dataset is crucial, providing a rich historical record of access control decisions, encompassing data from around 9000 users and 7000 resources, culminating in over 32,000 authorization records. Each record contains detailed metadata, including eight user characteristics, a resource identifier, and a binary action label indicating approval permission (1) or rejection permission (0) of access requests. A notable aspect of this dataset is its significant class imbalance, with approximately 93% of the records indicating granted access, highlighting the challenges in accurately analyzing and predicting access control decisions. As depicted in Fig. 3, the distribution within the dataset shows that grants are more prevalent than rejections, illustrating an imbalanced dataset.

The dataset consists of ten attributes: ACTION, RESOURCE, MGRID, ROLE1, ROLE2, ROLE3, ROLE4, ROLE5, ROLE6, and ROLE7. The label attribute is ACTION, as shown in Fig. 4. Additionally, the imbalance is especially noticeable, as class 0 (rejections) accounts for approximately 6% of the data (30,872 approvals compared to 1897 rejections). In order to address this imbalance and improve the model's ability to learn from the minority class, we utilised stratified sampling for K-fold cross-validation and applied class weights during the training of the model. This methodology guarantees a fair and balanced contribution from both classes to the loss function, thereby improving the performance of the model on this imbalanced dataset.

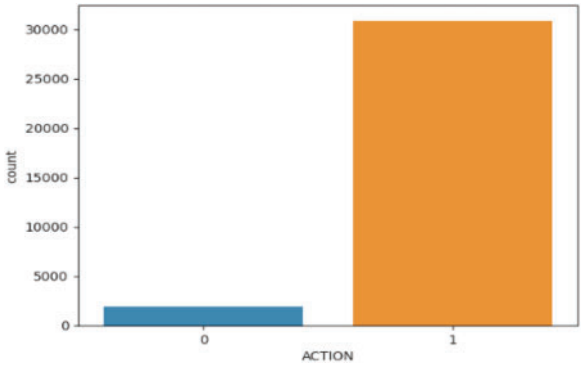

Figure 3: Distribution of target variable before data balancing

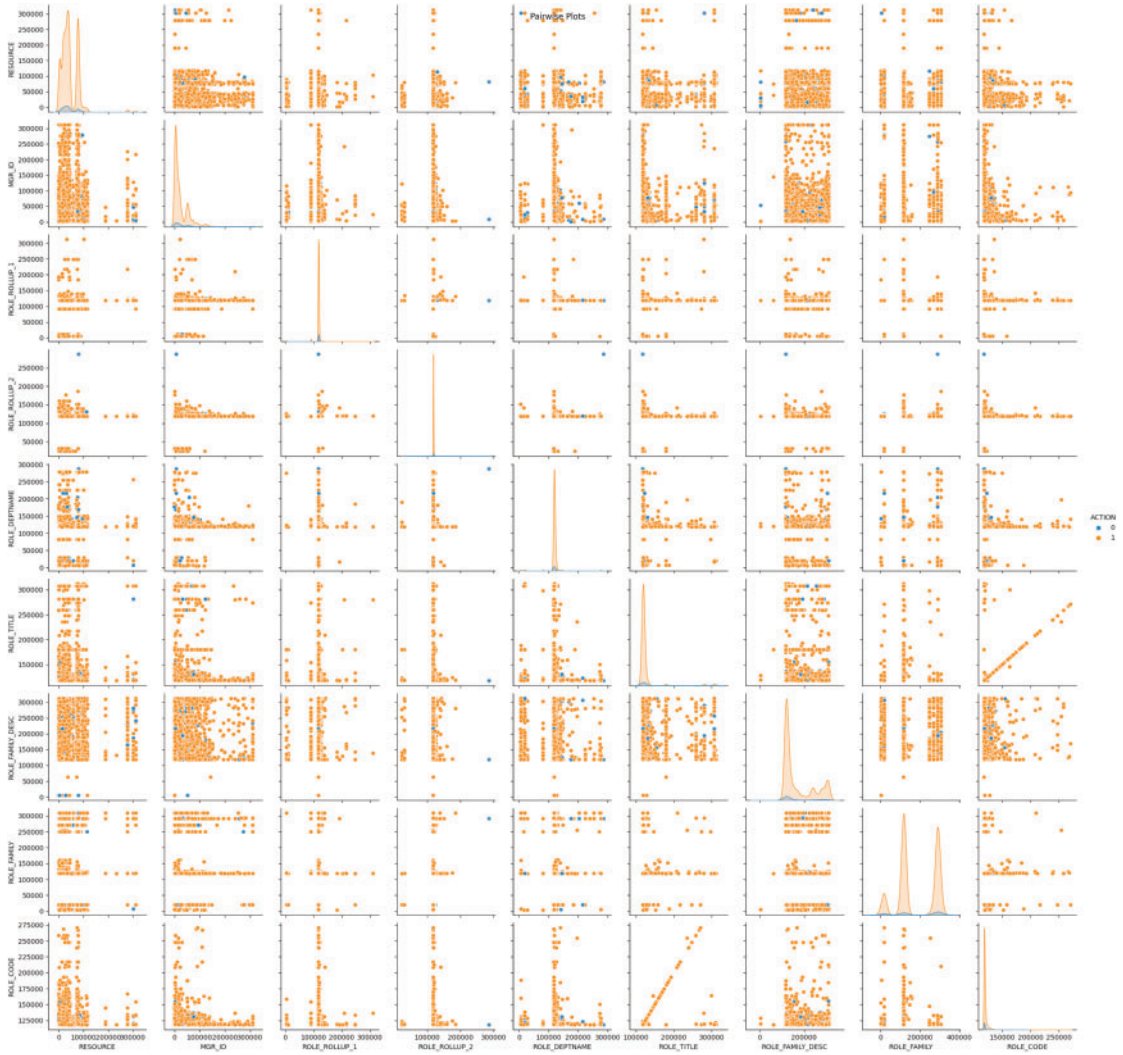

Figure 4: Features of amazon access control policy datasets

Furthermore, the experimental dataset was divided into training (80%) and testing (20%) subsets, and data balancing techniques were implemented to achieve a more equitable distribution of classes. The analysis was performed on a Mac operating system equipped with an M1 chip, 64 GB of memory, and Python version 3.10. This demonstrated the practicality of using advanced machine learning techniques to tackle the difficulties posed by imbalanced datasets in the field of access control policy analysis. In Table 2, we provide more detailed technical explanations regarding the implementation of the proposed model and the experimental setup.

Table 2: Components and setup for deep learning model in access control decision-making

Component	Details
Input layer	Takes in feature vectors from access request metadata, including user and resource attributes.
Hidden layers	Three hidden layers with 256 neurons each, using ReLU activation function.
Output layer	Single neuron with a sigmoid activation function, outputs a probability score for granting access.
Data preprocessing	Handled missing values, encoded categorical variables, normalized the dataset.
Dataset split	80% training, 20% validation.
Loss function	Binary cross-entropy loss.
Experimental setup	Dataset: Kaggle Amazon access control policy dataset with 32,000 records.
Data balancing	Class weighting to handle imbalance (93% granted *vs.* 7% denied).
Software/Hardware	Mac with M1 chip, 64 GB of memory, Python 3.10.

4.2 Performance Evaluation Criteria

The efficacy of the suggested solution in enhancing access decisions within access control was assessed based on the subsequent performance criteria: The evaluation included the development of a confusion matrix, as demonstrated by the correlation matrix shown in Fig. 5.

In this matrix, D_{AA} represents the count of samples where access requests were incorrectly granted, D_{AR} represents the count of samples where access requests were incorrectly denied, D_{RA} represents the count of samples where access requests were incorrectly allowed, and D_{RR} represents the count of samples where access requests were incorrectly rejected, as shown in Table 3, which was derived from the results of the access decision implementation.

- **Accuracy:** The accuracy measure evaluates the effectiveness of access control mechanisms in implementing access decisions in all possible situations. The percentage can be calculated by dividing the number of correct forecasts by the entire number of expectations. The subsequent equation of the confusion matrix is used to calculate accuracy.

$$Accuracy = \frac{D_{AA} + D_{RR}}{D_{AA} + D_{AR} + D_{RA} + D_{RR}} \tag{9}$$

- **Precision:** It refers to access decision accuracy and precision. The metric measures the system's ability to accurately identify and authorise authorised users while denying unauthorised ones. The precision metric is calculated by dividing the total number of positive samples by the number of correctly determined positive ones, where each positive data is accurate or incorrect. Dividing the total valid samples allowed by the expected number gives precision. The following

formula was utilised to determine it:

$$Precision = \frac{D_{AA}}{D_{AA} + D_{RA}} \tag{10}$$

- **Recall:** Evaluates the system's ability to effectively identify and include all occurrences of positive cases (authorized users) while minimizing the occurrence of false negatives (denying access to legitimate users). This metric assesses the model's capacity to accurately identify samples and is directly related to the size of the sample. The main objective of recall is to accurately categorize samples, and it remains stable even when flawed samples are incorrectly categorized. Even if the model incorrectly classifies all incorrect samples as correct, the recall rate will still be 100%. Recall calculation disregards negative samples, irrespective of their classification, as it solely focuses on genuine samples. The recall is determined by dividing the count of accurately identified positive samples by the overall count of positive samples and the subsequent equation was employed:

$$Recall = \frac{D_{AA}}{D_{AA} + D_{AR}} \tag{11}$$

- **F1 score:** The F1 score metric considers precision (rate of correctly identified authorised users to all users identified) and recall. The F1 score evaluates both aspects of the access control system's ability to make accurate access decisions. Formula used to calculate it:

$$F1Score = \frac{Precison * Recall}{Precision + Recall} \tag{12}$$

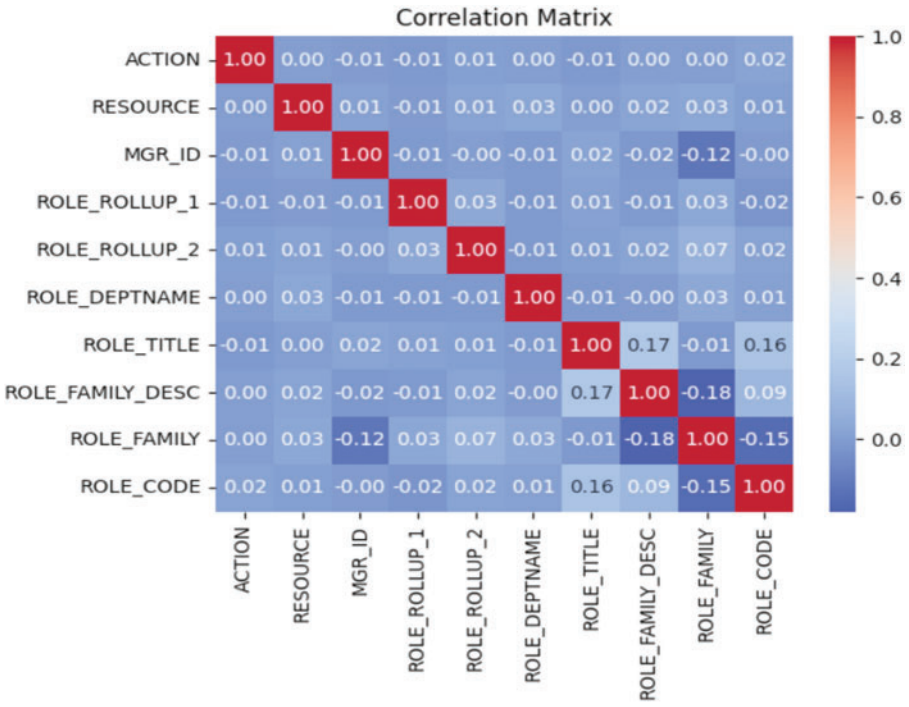

Figure 5: Correlation matrix

Table 3: Confusion matrix of security access decision enforcement results

	Predicted outcomes	
Real outcomes	Allowed access	Refused access
Allowed access request	D_{AA}	D_{AR}
Refused access request	D_{RA}	D_{RR}

5 Results Analysis

This section provides an analysis of the results obtained from the implementation of the access decision enforcement methodology using different deep learning techniques. Moreover, it evaluates the performance results of various deep learning techniques, encompassing both the fundamental and combined models, in efficiently handling access determinations in intricate and ever-changing environments like BYOD. The study employs basic deep learning models, such as the Multi-Layer Perceptron (MLP), and investigates combined models such as the LSTM-GRU Hybrid, Conv1D-GRU Hybrid, Conv1D-RNN Hybrid, Multi-Channel Conv1D (MConv1D) RNN-Dense, and Tabular DNN Models. The study specifically examines how these models perform in handling imbalanced datasets. The assessment of these models relies on a comprehensive range of metrics, including accuracy, precision, recall, F1 score, AUC (Area Under the Curve) score, training loss, and validation loss.

5.1 Performance Analysis of Access Decision Enforcement Based on Classical Deep Learning Model

This section examines the outcomes of implementing the access decision through the utilisation of fundamental deep learning techniques, specifically Multi-Layer Perceptron (MLP). To illustrate, Table 4 presents the performance metrics of four MLP models with varying complexity, ranging from 1 to 4 layers. Notably, all scenarios demonstrate a high level of accuracy, precision, recall, and F1 scores, indicating that they perform similarly in correctly implementing the access decision and maintaining a balance between precision and recall. Nevertheless, there is a small difference in the AUC scores, with the single-layer model achieving the lowest AUC of 0.62, while the four-layer model achieves the highest AUC of 0.65.

Table 4: Performance evaluation of access decision enforcement based on MLP models across various layer configurations

Methods	Accuracy	Precision	Recall	F1 score	AUC score
MLP 1 layer	0.94	0.96	0.99	0.97	0.62
MLP 2 layer	0.94	0.96	0.98	0.97	0.64
MLP 3 layer	0.94	0.96	0.98	0.97	0.63
MLP 4 layer	0.94	0.96	0.98	0.97	0.65

Although the models have high accuracy and other metrics, the relatively lower AUC scores indicate that they may not be as effective in differentiating between approved and denied access decision enforcement. This issue may expose a constraint in the models' capacity to generalise or indicate overfitting, as a model that predicts the majority class accurately but struggles with the minority class can sometimes yield high precision and recall. Moreover, the rise in AUC (Area Under

the Curve) as more layers are added indicates a marginal enhancement in the model's capacity to generalise as its complexity grows. Nevertheless, the consistently low AUC scores across all models suggest that this particular aspect may need additional focus and enhancement.

The illustrations in Fig. 6 depict the efficacy of various Multi-Layer Perceptron (MLP) configurations in enforcing access decision enforcement, with varying layer depths during the training phase. Specifically, the performance is measured by the Area Under the Curve (AUC) and the progression of loss metrics for both the training and validation phases. For instance, the AUC of the training model for the MLP with a single layer initially starts at a high value and remains stable, demonstrating an excellent match to the training dataset. Nevertheless, the validation area under the curve (AUC) demonstrates a decrease following an initial increase, indicating a propensity for overfitting. This observation is further corroborated by the loss plot, in which the validation loss exhibits an upward trend after the second epoch, in stark contrast to the decreasing trend observed in the training loss. In a similar way, the Multilayer Perceptron (MLP) with two layers exhibits a comparable trend in Area Under the Curve (AUC). Specifically, the AUC for the training data reaches a plateau while the AUC for the validation data decreases after an initial rise, suggesting the possibility of overfitting. Moreover, the loss plot confirms this observation, displaying a decrease in training loss but an increase in validation loss after the initial epoch.

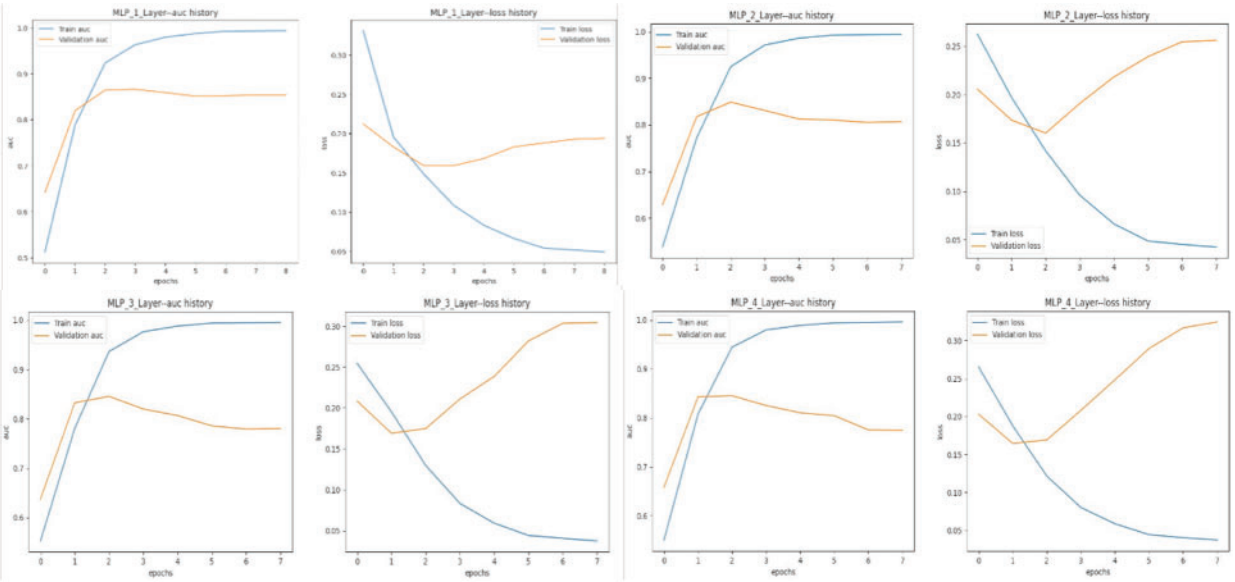

Figure 6: Comparative analysis of training and validation AUC for access decision enforcement based on MLP models with different layers and data balancing techniques

Similarly, for the MLP with three layers, the AUC history suggests overfitting as the validation AUC decreases after the first epoch. The loss plot clearly demonstrates a noticeable divergence between the training and validation loss after the initial epoch, further indicating overfitting. Additionally, the issue of overfitting persists in the MLP with four layers, as evidenced by a substantial decrease in validation AUC after the initial epoch. The loss history also shows a significant rise in validation loss after an initial decrease, suggesting a decline in the model's capacity to generalize to new access requests.

Upon comparing all four models, it becomes apparent that each model exhibits early overfitting during the training process. This is indicated by the rise in validation loss and the decline in validation AUC. Consequently, these findings suggest that simplifying the model, implementing regularization techniques, or stopping training early could improve generalization. Furthermore, the extent of overfitting worsens as the model's complexity escalates with the inclusion of extra layers.

5.2 Performance Analysis of Access Decision Enforcement Based on a Hybrid Model

This section provides an examination of the results obtained from implementing the hybrid deep learning approach to enforce access decisions. The performance evaluation includes four separate models, which are described in detail in Table 5. The results clarify that among the various hybrid models analysed, the Conv1d_RNN_Hybrid model stands out as significantly superior, demonstrating higher levels of Recall, Accuracy, AUC Score and F1 score.

Table 5: Comparative performance evaluation of access decision enforcement based on hybrid models

Methods	Accuracy	Precision	Recall	F1 score	AUC score
LSTM	0.25	0.96	0.21	0.34	0.52
LSTM GRU hybrid	0.32	0.95	0.30	0.38	0.52
Conv1d GRU hybrid	0.46	0.95	0.45	0.58	0.51
Conv1d RNN hybrid	0.82	0.95	0.85	0.89	0.54
Conv1d RNN dense	0.65	0.95	0.66	0.72	0.58

In contrast, the LSTM_1_Layer approach exhibits subpar performance in terms of Accuracy and Recall, indicating its difficulty in accurately detecting occurrences of the positive category. The Conv1d_RNN_Hybrid model demonstrates superior performance compared to both the LSTM_GRU_Hybrid and Conv1d_GRU_Hybrid models in these areas, while the latter two models exhibit some enhancements. Considering that the Conv1d-based hybrids performed better than the LSTM-based method, it is evident that including a Conv1d layer is advantageous. Integrating a Dense layer into the Conv1d_RNN approach Conv1d_RNN_Dense enhances the AUC Score and maintained Precision, while diminishing the Accuracy and F1 score in comparison to the Conv1d RNN hybrid method. Based on this finding, it seems that the overall precision of the Conv1d_RNN_Dense algorithm is relatively low, despite its strong performance in ranking instances that are positive.

Four different tiers of hybrid neural network models are shown in Fig. 7 along with their respective areas under the curve (AUC) and loss statistics. The AUC scores of the LSTM_GRU model are not constant, indicating that its performance varies across epochs. While the Conv1d_GRU model does improve the AUC metric, there is no proportional reduction in the validation loss compared to the training loss, suggesting overfitting. Consistently improving area under the curve (AUC) and convergent loss values indicate robust generalizability, which is valid for the Conv1d_RNN model. A validation-training loss discrepancy suggests overfitting in the MLP_3_Layer model, even though it has a high training AUC. The Conv1d_RNN hybrid model achieves a better balance between learning and generalization than other models.

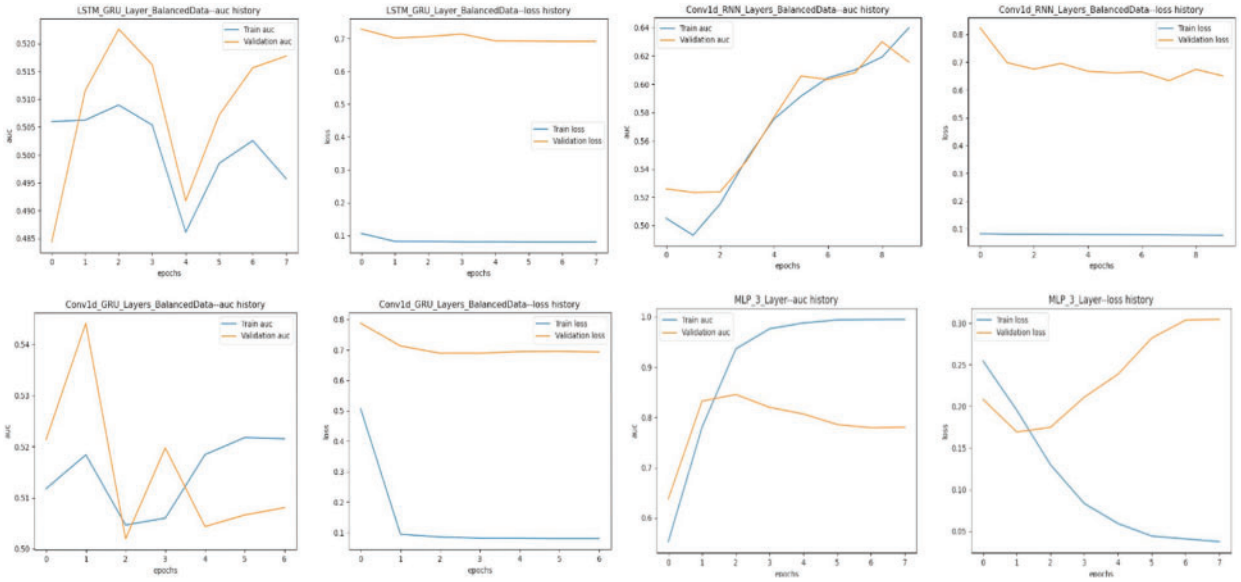

Figure 7: Comparative analysis of training and validation AUC metrics for access decision enforcement based hybrid models

5.3 Performance Analysis of Access Decision Enforcement Baesd on TabularDNN Models

Additionally, this section uses Tabular Deep Neural Network (TabularDNN) metrics to examine the performance outcome of access decision execution. Effective learning in correctly implementing access decisions is demonstrated by the general trend of improving training accuracy and lowering training loss, as shown in Fig. 8, which displays the training and validation accuracy and losses across epochs for each model configuration. Specifically, the three-layer, 256-neuron configuration outperforms its competitors regarding validation loss reduction, implying better generalization capabilities. Furthermore, Table 6 shows distinct findings about the Area Under the Curve (AUC) scores and other performance metrics such as precision, recall, and F1 scores. Moreover, the single-layer TabularDNN model shows the highest area under the curve (AUC) score among the configurations lacking the specification of 256 neurons, indicating superior class differentiation. In contrast, models with increasing stratification, specifically two- and three-layer configurations, show little reduction in AUC scores, implying potential overcomplexity without commensurate gains in discriminatory power. Ultimately, the AUC result improves significantly when 256 neurons are added to a three-layer setup, indicating optimal performance. Despite the minor differences in AUC scores, all models perform well when it comes to accurately implementing access decisions, with high precision, recall, F1, and precision scores exceeding 0.94.

The juxtaposition of the graphical training histories with the tabulated performance metrics shows that although the precision, precision, recall, and F1 scores remain consistently high across configurations, the AUC score provides a more accurate view of the model's effectiveness, particularly in distinguishing between an accept or reject access decision. The three-layer model with 256 neurons has slightly better generalization ability, as demonstrated by the validation loss path and superior AUC score. This comparison underscores the importance of considering multiple performance dimensions when evaluating and selecting model configurations for optimal generalization of new access requests.

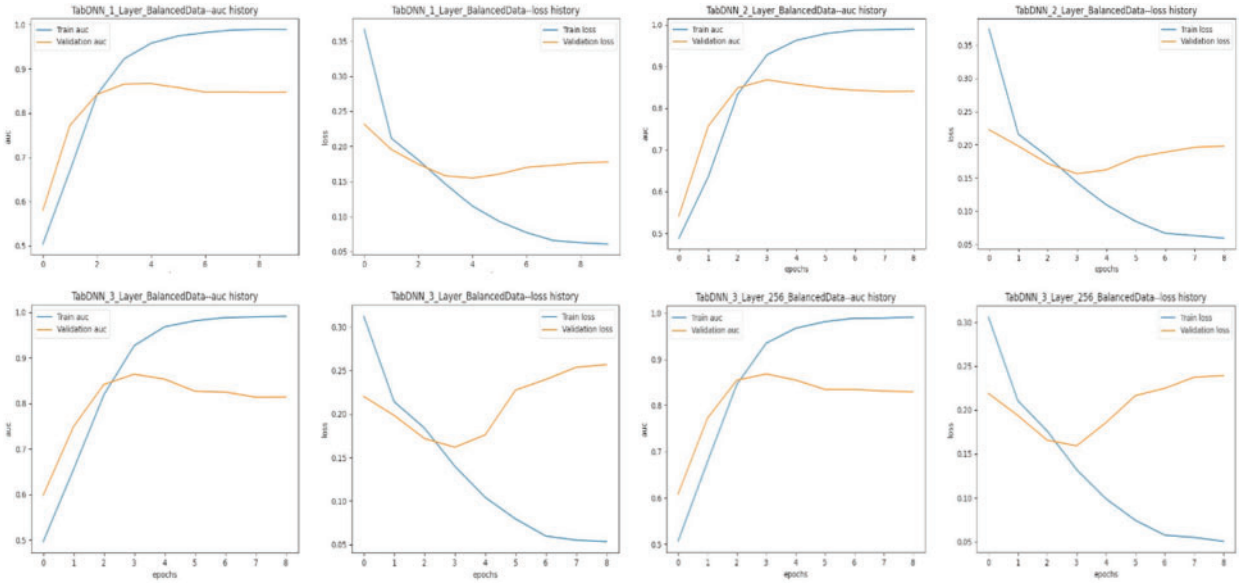

Figure 8: Comparative analysis of training and validation metrics for tabular deep neural networks with different layers and data balancing techniques

Table 6: Performance evaluation of access decision enforcement based on TabularDNN models across various layer configurations

Methods	Accuracy	Precision	Recall	F1 score	AUC score
TabularDNN 1 layer	0.94	0.96	0.99	0.97	0.85
TabularDNN 2 layer	0.94	0.96	0.98	0.97	0.84
TabularDNN 3 layer	0.94	0.96	0.98	0.97	0.83
TabularDNN 3 layer 256	**0.94**	**0.96**	**0.98**	**0.97**	**0.86**
TabularDNN 4 layer	0.94	0.96	0.98	0.97	0.85

6 Discussion

Access control decision enforcement in Bring Your Own Device (BYOD) environments faces critical challenges and limitations. Traditional mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), enforce access based on roles or attributes. While valuable, these approaches are rigid due to their reliance on predefined policies and specific attributes, struggling with the dynamic nature of access control. Minor changes in user and resource properties can significantly impact access control status, creating challenges for system administrators. This necessitates complex rules with numerous conditions and permissions, leading to policy conflicts, decision-making bottlenecks, delayed access response times, and suboptimal performance.

Machine learning-based access decision enforcement methodologies provide increased flexibility. However, they require extensive attribute engineering and policy formulation, leading to increased access response times, performance bottlenecks, and inadequate adaptiveness. The proposed methodology addresses these challenges by offering an adaptive and dynamic access control decision

enforcement approach using multi-layer hybrid deep learning techniques, specifically TabularDNN, to improve the flexibility and responsiveness of access control systems.

The proposed solution eliminates the need for feature engineering by directly utilizing metadata from access requests. It employs a trained deep neural network to swiftly make access control decisions based on user and resource metadata, overcoming the limitations of current systems. By analyzing multiple attributes of access requests across various layers using multilayer hybrid deep learning techniques, the solution ensures reliable and accurate access authorization. This approach enhances flexibility and dynamism by not depending on specific policies or limited attributes.

The methodology applies various basic and hybrid deep learning algorithms across multiple layers. The solution is implemented by balancing the dataset, constructing training and test models, and enforcing access decision mechanisms. To evaluate the effectiveness of the proposed solution, we use the Kaggle Amazon access control policy dataset and conduct several experiments. We estimate performance metrics by comparing efficiency across different deep learning algorithms and evaluate accuracy against previous methodologies. Experimental results indicate up to 94% accuracy in executing the access decision.

The proposed methodology offers several advantages compared to previous research. Cappelletti et al. [4] utilized historical access logs to improve decision-making processes, yet the time required for analyzing features within the logs may adversely affect performance. Khilar et al. [5] presented a trust-based mechanism leveraging machine learning to grant access to cloud resources. This method considers user behavior and authorization history, employing random forest and k-NN algorithms, achieving an accuracy of 92.1% in access decision-making. Despite its advantages, this approach has inherent limitations. The effectiveness of decisions relies on user attributes in the access request, extending the time required to implement decisions and leading to potential performance bottlenecks in the access decision-making process.

Additionally, Srivastava et al. [6] developed a machine learning-based Risk Access Control (RAAC) system for making access decisions. This system employs the random forest algorithm, factoring in variables such as access time, location, frequency of requests, and resource sensitivity. This method demonstrated high effectiveness, but faced challenges related to decision time and feature engineering, impacting operational efficiency. Mingshan et al. [7] proposed a decision-making-based Boosting Window (BW) algorithm to construct an access control knowledge graph, achieving a performance accuracy of 89.64%. However, there remains a need to improve the performance of access decision-making further. In contrast, the proposed solution enforces access decision-making to a binary outcome—granting or denying access—based on a Tabular Deep Neural Network (TabularDNN) with a three-layer, 256-neuron configuration, emerging as the optimal choice for access decisions in this approach, exhibiting superior accuracy and efficiency in predicting access control decisions. In Table 7, previous studies are compared with the proposed solution in terms of techniques and benchmarks.

The method that was proposed outperformed other methodologies primarily due to the fact that it employs Tabular Deep Neural Networks (TabularDNN) that integrate multiple layers to conduct a nuanced analysis of user and resource attributes, thereby substantially improving adaptation and precision. It dynamically processes metadata from access requests, thereby reducing computational overhead and reducing the time from data ingestion to decision-making. This method, in contrast to conventional models that depend on static principles, employs dynamic and adaptable data processing, thereby avoiding the need for extensive feature engineering. The architecture effectively captures intricate relationships and patterns, allowing for rapid changes, such as updates to user roles or

policies, without the need for laborious recalibration. Additionally, its scalability guarantees consistent performance even as data volumes increase, making it an ideal choice for large organizations with intricate access scenarios. Additionally, it effectively manages non-linear relationships, which enhances the reliability and accuracy of access decisions.

Table 7: Comparative results of current and previous solutions in enforcing access decisions

Ref	Methodology	Performance
[4]	Utilized historical access logs to improve decision-making processes. It requires time-consuming feature engineering, limiting performance and adaptability.	NA
[5]	Presented a trust-based access decision enforcement mechanism leveraging machine learning to grant access to cloud resources(RF, k-NN). It requires time-consuming feature engineering, limiting performance and adaptability.	92.1%
[7]	Proposed a decision-making-based Boosting Window (BW) algorithm to construct an access control knowledge graph. It requires time-consuming feature engineering, limiting performance and adaptability.	89.64%
The proposed work	Access decision enforcement based on multilayer and hybrid method (TabularDNN). It is flexible, doesn't require specific features, and relies on user and resource metadata in the access request.	94%

The experimental results demonstrate the effectiveness of the proposed access decision enforcement based on hybrid deep learning techniques with multiple layers, achieving up to 94% accuracy in executing access decisions. This research significantly contributes to the field by presenting a deep learning-based model that enhances accuracy, dynamism, and flexibility in access decision implementation while simplifying administrative processes.

The proposed model is a substantial advancement in the enforcement of access decisions in BYOD environments. Nevertheless, it does demonstrate certain limitations. The quality and comprehensiveness of the metadata utilized for decision-making are critical to its efficacy. The accuracy of access control decisions may be affected by insufficient or substandard input data. Additionally, some hybrid deep learning models have limitations in handling complex and large datasets related to access requests, and they may face issues of overfitting and underfitting. To address these limitations, future research could explore alternative deep learning algorithms and techniques to enhance the scalability and applicability of the proposed methodology in diverse organizational settings. Additionally, future work will involve evaluating the model across various datasets and conducting cross-dataset validations to ensure its adaptability and reliability in different contexts.

7 Conclusions

As organizations embrace modern Bring Your Own Device (BYOD) technology, they face security challenges such as unauthorized access—traditional access control has limited effectiveness in a complex and dynamic environment. This study introduces an approach for enforcing access decisions using multi-layer hybrid TabularDNN technology, which converts user and resource attributes from access request metadata into granting or denying categories without extensive policy engineering.

The effectiveness of the solution was evaluated using Amazon Access Control Policy datasets. The solution's results achieved an accuracy of 94% in enforcing the access decision. The solution improves access control systems by enabling adaptation to changing attributes and complex, dynamic environments through basic and hybrid deep learning algorithms. Besides, it improves privacy by ensuring indirect communication between the access decision engine and the policy administration. Future efforts will involve testing the model on various datasets and validating its reliability and adaptability across scenarios.

Acknowledgement: The authors of this paper would like to thank the reviewers for their observations, comments, and suggestions for improving the manuscript's content. This work was supported in part by the University of Malaya Impact Oriented Interdisciplinary Research Grant under Grant IIRG008 (A, B, C)-19IISS.

Funding Statement: This work was partly supported by the University of Malaya Impact Oriented Interdisci-plinary Research Grant under Grant IIRG008 (A, B, C)-19IISS.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Aljuaid Turkea Ayedh M; data collection: Aljuaid Turkea Ayedh M; analysis and interpretation of results: Aljuaid Turkea Ayedh M; draft manuscript preparation: Aljuaid Turkea Ayedh M; supervision: Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used in this study is derived from the Kaggle Amazon access control policy dataset. The dataset includes comprehensive information on access control policies, which were essential for the analysis and results presented in this paper. No additional data was used in this study.

Ethics Approval: Not applicable. This study does not involve any biological or medical research requiring ethical approval.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] R. Palanisamy, A. A. Norman, and M. L. Kiah, "Compliance with bring your own device security policies in organizations: A systematic literature review," *Comput. & Secur.*, vol. 98, no. 1, Nov. 2020, Art. no. 101998. doi: 10.1016/j.cose.2020.101998.

[2] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "Preventing unauthorized access in information centric networking," *Secur. and Priv.*, vol. 1, no. 4, Aug. 2018, Art. no. e33. doi: 10.1002/spy2.33.

[3] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access control for IoT: A survey of existing research, dynamic policies and future directions," *Sensors*, vol. 23, no. 4, Feb. 2023, Art. no. 1805. doi: 10.3390/s23041805.

[4] L. Cappelletti, S. Valtolina, G. Valentini, M. Mesiti, and E. Bertino, "On the quality of classification models for inferring abac policies from access logs," in *2019 IEEE Int. Conf. on Big Data (Big Data)*, Los Angeles, CA, USA, IEEE, Feb. 2019, pp. 4000–4007.

[5] P. M. Khilar, V. Chaudhari, and R. R. Swain, Trust-based access control in cloud computing using machine learning. in *Cloud Computing for Geospatial Big Data Analytics*. Springer, Dec. 2019, pp. 55–79.

[6] K. Srivastava and N. Shekokar, "Machine learning based risk-adaptive access control system to identify genuineness of the requester," in *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough*. Springer, Feb. 2020, pp. 129–143.
[7] M. You, J. Yin, H. Wang, J. Cao, and Y. Miao, "A minority class boosted framework for adaptive access control decision-making," in *Int. Conf. Web Inform. Syst. Eng.*, Springer, Jan. 2021, pp. 143–157.
[8] J. E. Lee, S. H. Park, and H. Yoon, "Security policy based device management for supporting various mobile os," in *2015 Second Int. Conf. Comput. Technol. and Inform. Manag. (ICCTIM)*, Johor, Malaysia, IEEE, Apr. 2015, pp. 156–161.
[9] K. Yanson, "Results of implementing WPA2-enterprise in educational institution," in *2016 IEEE 10th Int. Conf. Appl. Inform. and Commun. Technol. (AICT)*, Baku, Azerbaijan, IEEE, Jul. 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 *2016 IEEE Int. Conf. Comput. Sci. Eng. (CSE) and IEEE Int. Conf. Embed. Ubiquitous Comput. (EUC) and 15th Int. Symp. on Distrib. Comput. Appl. Business Eng. (DCABES)*, Paris, France, IEEE, Jul. 2016, pp. 557–560.
[11] O. Oluwatimi, M. L. Damiani, and E. Bertino, "A context-aware system to secure enterprise content: Incorporating reliability specifiers," *Comput. & Secur.*, vol. 77, no. 3, pp. 162–178, Aug. 2018. doi: 10.1016/j.cose.2018.04.001.
[12] B. L. D. Seneviratne and S. A. Senaratne, "Integrated corporate network service architecture for bring your own device (BYOD) policy," in *2018 3rd Int. Conf. Inform. Technol. Res. (ICITR)*, Moratuwa, Sri Lanka, IEEE, Jun. 2018, pp. 1–6.
[13] C. C. Chang, I. C. Lin, and C. T. Liao, "An access control system with time-constraint using support vector machines," *Int. J. Netw. Secur.*, vol. 2, no. 2, pp. 150–159, Oct. 2006.
[14] L. Karimi, M. Abdelhakim, and J. Joshi, "Adaptive abac policy learning: A reinforcement learning approach," May 2021, *arXiv:2105.08587*.
[15] M. Ayedh, T. Aljuaid, A. W. Wahab, and M. Y. Idris, "Enhanced adaptable and distributed access control decision making model based on machine learning for policy conflict resolution in BYOD environment," *Appl. Sci.*, vol. 13, no. 12, Jun. 2023, Art. no. 7102. doi: 10.3390/app13127102.
[16] T. Bui and S. D. Stoller, "A decision tree learning approach for mining relationship-based access control policies," in *Proc. 25th ACM Symp. Access Control Models and Technol.*, Jun. 2020, pp. 167–178.
[17] T. Bui, S. D. Stoller, and H. Le, "Efficient and extensible policy mining for relationship-based access control," in *Proc. 24th ACM Symp. on Access Control Models and Technol.*, May 2019, pp. 161–172.
[18] L. Karimi, M. Aldairi, J. Joshi, and M. Abdelhakim, "An automatic attribute-based access control policy extraction from access logs," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2304–2317, Jan. 2021. doi: 10.1109/TDSC.2021.3054331.
[19] A. Jabal *et al.*, "Polisma–a framework for learning attribute-based access control policies," in *Comput. Secur.–ESORICS 2020: 25th European Symp. Res. Comput. Secur., ESORICS 2020*, Guildford, UK, Springer, Sep. 2020, pp. 523–544.