A Hybrid Data Protection Mechanisms Using Attribute Based Encryption and Role Based Access Control Mechanism for Digital Music Classrooms

Lina Song

Public Arts Education and Teaching Center, Zhongyuan Institute of Science and Technology, Zhengzhou 451400, China
E-mail: lnasong@outlook.com

Received 16 July 2025; Accepted 28 August 2025

Abstract

Network Security in Cloud-Based Digital Music Classrooms (NS-CDMC) is a novel architecture that secures critical educational environments. RBAC, fine-grained ABE, dynamic TBAR, secure session creation, data integrity verification, and proactive anomaly-based intrusion detection are used in NS-CDMC. The NS-CDMC model has demonstrated superior performance across critical security metrics compared to several benchmark methods. Key results include an Anomaly Detection Rate (ADR) of 0.96, outperforming other methods and indicating the model's ability to detect sophisticated threats and insider misuse. The model handles access requests efficiently with an Access Control Decision Latency of 48 ms, comparable to or lower than other benchmark techniques. Additionally, the NS-CDMC model has a substantially lower False Positive Rate (FPR) of 0.03, minimizing unnecessary interruptions and improving operational smoothness in digital music classrooms. Simulations for the NS-CDMC model captured access choices,

Journal of Cyber Security and Mobility, Vol. 14_5, 1033–1066.
doi: 10.13052/jcsm2245-1439.1451

trust score changes, anomaly scores, and Attribute-Based Encryption (ABE) policy applications. The NS-CDMC security framework provides a secure, real-time, and user-friendly environment for digital music classrooms using ABE, Trust-Based Access Refinement (TBAR), and anomaly detection. ABE restricts content decryption to authorized users based on roles, courses, and instruments. TBAR dynamically adjusts access control based on user trust scores, which reflect behavior in the system.

Keywords: Cloud security, digital music classrooms, access control, data protection, network security, role-based access control (RBAC), attribute-based encryption (abe), secure data storage, intrusion detection and anomaly detection.

1 Introduction

The world of higher education has changed a lot. Digital music assets are one-of-a-kind, typically copyrighted, and contain very sensitive performance data and exclusive instructional materials. Because of this, they need a security architecture that is more advanced than standard business solutions. There are a lot of common security holes on broadband networks, especially the Internet, which is where cloud computing services are hosted [1, 2]. As these systems get better, their security threats go up. Cloud computing is different from regular computing in many ways, such as its openness, distributed processing and storage, borderless access, virtualization, multi-tenancy, and the fact that data ownership and management rights are separate [3]. But the new way of doing things has people worried about security. The cloud has a lot of data and a complicated system architecture since it includes so many different applications, services, and standards. This is a challenge for security on the technological, administrative, and legal levels. Hackers go for the cloud because it houses private consumer information [4]. Security is very important since an attack on a cloud system might cost cloud service providers and customers a lot of money. Cloud security is different from regular IT security. Their main concern is the security of cloud computing platforms. The cloud's openness and growth make it easier for hackers to get in and steal data [5, 6]. Second, the virtualization layer makes it harder to separate and safeguard workloads, which puts tenant environments at risk. Separating data ownership from management rights makes it harder to find and keep track of security incidents, which raises the dangers of cloud computing security [7].

Hackers are drawn to cloud computing systems because they have a lot of users and data, which makes them more likely to be attacked [8, 9]. A breach might get worse and damage other sites. Because the interface is open, security has to be very tight. Another issue is keeping safe the information resources that cloud computing tenants share [10]. The virtual world makes both technology and administration harder. Traditional physical security perimeters don't work to safeguard shared virtualized user apps and data. It is hard to find failures in cloud computing systems since they are so big and employ virtual computers to do their work [11, 12]. Cloud computing's new service paradigm separates ownership, administration, and empowerment of resources. Decoupling makes it harder for consumers to manage physical resources, which makes them more vulnerable to security holes in the service provider [13, 14].

NS-CDMC is a real-time access control system that combines traditional access control techniques with cutting-edge data security and threat intelligence. To begin, we will begin by making the primary components of the system, which include users, roles, permissions, and resources, more formal. Next, we will discuss a layered access control technique that combines Role-Based Access Control (RBAC) for structured permission management with Attribute-Based Encryption (ABE) for securing data at a very high level. This method is referred to as a layered access control architecture. It is essential to have this model because it demonstrates how to protect data while it is being sent and stored, how to establish secure communication channels by using a protocol that is similar to TLS, and how to establish an anomaly-based intrusion detection system that monitors how employees behave. We implemented a comprehensive audit logging system that makes use of hash chains to guarantee that security data cannot be altered in any way. The goal of the proposed NS-CDMC model is to provide a security posture for cloud-based digital music education that is robust, simple to verify, and adaptable at any time.

2 Literature Review

Conventional and modified conventional recommendation algorithms are the major recommendation system approaches. In artificial intelligence, recommendation algorithms, deep learning, and reinforcement learning have evolved. Traditional recommendation algorithms have connected the past and future throughout recommendation system development, and all emergent algorithms have improved and innovated on them. Under artificial

intelligence, the recommendation system has brought ongoing prosperity. Traditional, enhanced, and neural network-based recommendation algorithms that employ deep learning for deep feature extraction are the primary topics of recommendation algorithm research. Reinforcement learning-based recommendation algorithms replicate the suggestion process to enhance accuracy and variety. A hybrid recommendation system based on attribute weights on user importance was proposed by Debnath et al. [15] after analyzing current recommendation algorithms. The algorithm model improves the recommendation system by balancing the two algorithms' strengths and downsides. An LDA and Shannon distance-based content-based recommendation architecture by Bagul et al. [16] delivers query-time document-like recommendations. He et al. [17] proposed neural network-based collaborative filtering that embeds user data using MF and learns user-item interaction data using MLP. Chen et al. [18] proposed a context-based image recommendation method that transfers image pixels to the context for customized image recommendations. Selmene et al. [19] proposed a user sentiment analysis-based recommendation system that used sentiment data in collaborative filtering and item average ratings to substitute missing rating matrix values to improve suggestion accuracy. A time-perception-based music recommendation system incorporating implicit feedback and temporal dynamics was proposed by Sánchez et al. [20].

Recent studies have shown how useful context-aware access control systems are in cloud and fog networks. Kayes et al. [21] thoroughly examined context-aware access control techniques. Access control systems must adapt to context and user behavior, they said. Their taxonomy and open research issues provide the groundwork for future investigation. A student may only require access to a music sheet during class, or a teacher's access privileges may alter depending on whether they are teaching or assessing. To answer experts' main concerns, Kayes et al. is used to demonstrate that the new ABE+RBAC model is theoretically sound and handles real-world contextual rules well.

Zhang et al. [22] created a fast, privacy-preserving decentralized Attribute-Based Encryption (ABE) method for expressive access models. Their approach secures and details decentralized access management while protecting users' private keys. This research shows how ABE can safeguard cloud-based private data. Zhang et al.'s work demonstrates that the cryptographic part of the new hybrid model is not only functional but also competitive with and relevant to current advancements in encryption technology. Schummer et al. [23] created, tested, and evaluated a machine learning-based

network abnormality detection method. Their method successfully identified flaws and made the network safer. This research shows how machine learning can protect networks and identify complicated assaults. Besides rules (RBAC) and encryption (ABE), a full security system must incorporate dynamic risks that overcome static rights, such as a rogue authorized user against compare your proactive protection against a reactive, behavior-based detection solution, the model proposed by Schummer et al. is used. This comparison shows how broad your model is and why its hybrid approach offers strong security, even without ML-based threat detection.

Ogwara et al. [24] developed MINDPRES, a hybrid prototype system that protects all data on the mobile cloud's user layer. Their system uses a number of security methods to protect user data and make sure that it is sent safely. This research shows how important it is for mobile cloud platforms to have strong data security. Ogwara et al. provides an architectural benchmark. The comparison here is not just about one component, but about the overall design. The new paper would compare its ABE+RBAC hybrid architecture to MINDPRES's multi-layered system to argue that its design is comprehensive, efficient, and well-suited for its specific application (Digital Music Classrooms) when compared to other existing hybrid security frameworks. Fan et al. [25] proposed a deep adversarial society-based recommendation technique that moves user information between social and commodities domains via bidirectional mapping and adversarial learning. Music recommendation research uses Gaussian mixture models, Bayesian networks, and hidden Markov models. To deliver personalized music suggestions, Zheng et al. [26] dynamically integrated tag information and track temporal into user-item interaction. WMF is Hu et al.'s [27] customized TV show recommendation system. This method is becoming common for music recommendations. Latent factor suggestion helped Liu et al. [28] offer video background music. The recommended scoring algorithm uses the weighted average of video and music latent components. Stochastic gradient descent optimizes the pairwise-ranked objective function. A hidden Markov model identified music sequences and proposed personalized music by Li et al. [29]. Using k-nearest neighbor graph visualization in high-dimensional domains, Flexer et al. [30] studied how centrality influences real-world music recommendation systems Mutual proximity graphs reduce centrality and increase accessibility. Studies have also transformed audio data into bag-of-words music selection representations [31].

Table 1 presents a review for cloud security and educational technology, focusing on the proposed solution, which highlights key research gaps. This

Table 1 Review for cloud security and educational technology

Literature Domain	Key Findings & Contributions	Identified Gaps
Cloud Security (General)	– **RBAC** is a standard for access management, simplifying permissions by assigning them to roles. It's effective for general administrative control and enforcing the principle of least privilege.	– **Rigidity and lack of granularity**: RBAC can lead toarole explosion" in complex environments. It often can't enforce access based on dynamic conditions or data content. It is coarse-grained and struggles with complex policies.
Educational Technology	– Cloud computing is widely adopted in education for its scalability, cost-effectiveness, and collaboration features. – It enables new learning modalities, such as online music platforms, virtual classrooms, and shared digital resources.	– **Security is a major concern**: While cloud tech improves accessibility, it introduces significant risks related to data privacy, student records, and intellectual property. – **Lack of domain-specific solutions**: Most educational cloud security research is generic and doesn't address the unique, sensitive nature of data in specialized fields like digital music.
Digital Music Education	- Cloud-based platforms for music education improve access to tools and resources for composition, practice, and collaboration. – They allow for the creation and sharing of large, rich media files (audio, scores, projects).	– **Vulnerability of creative data**: The intellectual property (IP) of students and faculty—such as original compositions or performance recordings—is highly sensitive but not adequately protected at the data level. – **Inadequate security models for hybrid access**: Existing systems lack a fine-grained, policy-driven approach to protect these specific data types. An instructor may have general access to a student's project, but the system cannot restrict them from, for example, accessing the master audio file after the course ends.

(*Continued*)

Table 1 Continued

Literature Domain	Key Findings & Contributions	Identified Gaps
Attribute-Based Access Control (ABAC/ABE)	– ABAC/ABE offers fine-grained control by using a set of attributes to define access policies. – It's more flexible than RBAC and can handle dynamic, complex authorization decisions (e.g., "only allow access if the user is a 'student' AND their 'course' is 'Advanced Composition"').	– **Complexity of implementation**: ABE is computationally intensive and can be complex to manage, especially with a large number of attributes and policies. – **Administrative overhead**: Building and maintaining complex ABE policies without a foundational role-based structure can be challenging and prone to errors.

hybrid data protection mechanism aims to solve the limitations of current cloud-based education systems, especially within a specialized domain like digital music classrooms.

The suggested Hybrid Data Protection Mechanism directly tackles the problems found in the literature by making a system that works together to incorporate the best parts of RBAC and ABE. RBAC is fantastic for making administration more efficient, while ABE is great for protecting data in small amounts. However, they are generally seen as independent or competing models. The suggested approach combines them to provide a multi-layered security architecture, leveraging RBAC for initial access rights and ABE for content-level protection. The solution covers the need of securing sensitive, domain-specific intellectual property in digital music schools. It can build regulations that safeguard a student's composition, guaranteeing that only the student, the teacher, and potentially a chosen group of peers can decrypt and read the material, even if others have wide file-system access. RBAC is a basic layer that makes ABE much easier to manage. Administrators may govern access for a large number of users via roles (e.g., "Student," "Faculty," "Guest") while ABE handles the complicated, per-file security based on criteria like "Course ID," "Project Name," or "Grade Level." This avoids the "role explosion" issue of pure RBAC and the administrative complexity of pure ABE.

Traditional perimeter protections and static access lists fail in dynamic, distributed, and multi-tenant cloud systems. To combat increasingly sophisticated cyberattacks, network security must be proactive, layered, and intelligent. Current solutions focus on individual security aspects like access

control or encryption rather than a coherent, integrated strategy adapted to the operational and data sensitivity needs of specialized educational platforms like digital music classes. Security systems must detect threats and provide transparency and explainability, especially in academic settings where system administrators and end-users must understand "why" a security alert was triggered.

3 Proposed Method

This paper presents a model for NS-CDMC. The NS-CDMC model integrates several key cryptographic and access control mechanisms, alongside an anomaly detection system and audit logging, to protect sensitive educational resources and user interactions.

3.1 System Overview

The foundation of the NS-CDMC model begins with a clear definition of the system's core components:

- **Users (U):** This set encompasses all individuals interacting with the digital music classroom. It is denoted as $U = \{u_1, u_2, \ldots, u_n\}$, and includes distinct types such as students, instructors, and administrators.
- **Roles (R):** These are predefined categories that users can be assigned to, abstracting permissions. Examples include "Student," "Instructor," and "Admin." The set of roles is given by $R = \{r_1, r_2, \ldots, r_m\}$.
- **Permissions (P):** These define specific actions that can be performed within the system. Examples of permissions relevant to a digital music classroom might include "View" (for sheet music), "Upload" (for assignments), "Edit" (for collaborative projects), "Share" (for resources with other users), and "Download" (for learning materials). The set is $P = \{p_1, p_2, \ldots, p_k\}$.
- **Resources (RES):** This set represents all the digital assets available within the classroom. This could include musical scores, audio tracks, student feedback, lesson plans, virtual instrument configurations, and other class materials. It is denoted as $RES = \{res_1, res_2, \ldots, res_t\}$.

3.2 Role-Based Access Control (RBAC) Model

The NS-CDMC access control system is built on RBAC, which serves as the fundamental layer. By allocating permissions to roles rather than directly to

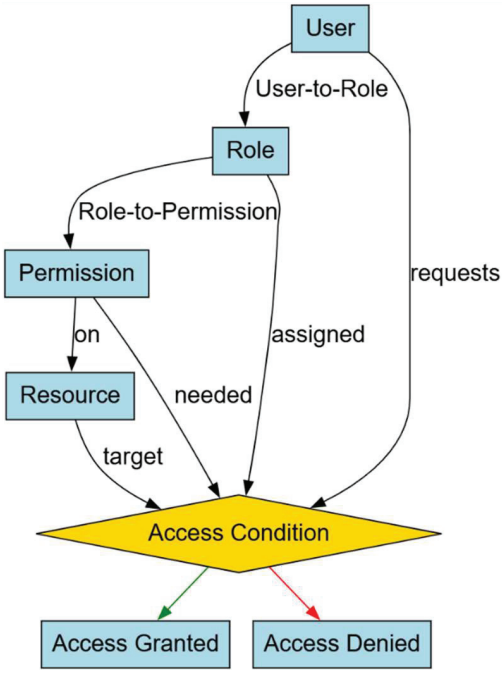

Figure 1 Role-based access control (RBAC) model.

individual users, it makes the administration of permissions more simpler. Figure 1 presents Role-Based Access Control (RBAC) Model.

The User-to-Role Assignment is something that is assigned to every user. The function assign: $\mathcal{U} \rightarrow 2^{\mathcal{R}}$, where $2^{\mathcal{R}}$ represents $\mathcal{R}$'s power set, allows users to be allocated a subset of all possible roles. Role-to-Permission Assignment allows access rights to different resources are defined by the roles that an individual can have. To indicate that a role has permissions for specified operations on resources, the function $perm : \mathcal{R} \rightarrow 2^{P \times RES}$ provides this mapping. Access Condition for a user u_i allows to have access to a resource res_j with a given permission p_k is that u_i be assigned a role r that includes the set of permissions for p_k and res_j such that,

$$\exists r \in assign(u_i)\text{: } (p_k, res_j) \in perm(r). \tag{1}$$

This RBAC structure ensures that access is managed systematically according to organizational roles, enhancing administrative efficiency and reducing the complexity of managing individual user permissions.

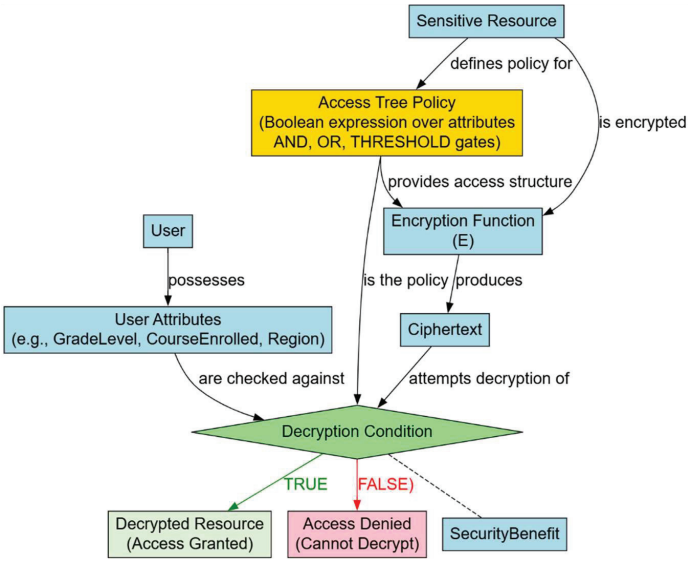

Figure 2 Attribute-based encryption (ABE).

3.3 Attribute-Based Encryption (ABE) for Fine-Grained Control

An extra layer of granular access control is provided by ABE (Fig. 2), which helps to further secure the privacy of sensitive information. ABE, on the other hand, determines which users are authorized to decrypt which data by using the specific qualities of those users, in contrast to RBAC, which limits the actions that users are allowed to carry out.

- User Attributes (A): "GradeLevel," "CourseEnrolled," and "Region" are some examples of descriptive qualities that are linked to users. It is denoted as $A = \{a_1, a_2, \ldots, a_q\}$. Each user u_i possesses a specific set of attributes $A_i \subseteq A$.
- Access Tree Policy (T): For each sensitive resource, an access policy is defined as a tree structure (or boolean expression) over attributes, using logical gates like AND, OR, and THRESHOLD. For instance, a resource might be accessible only if a user has "GradeLevel = Senior" AND "CourseEnrolled = Advanced Composition."
- Encryption Function: Each resource res_j is encrypted using an access structure T_j derived from the policy. The encryption function $Enc_{T_j}(\cdot)$ takes the resource and encrypts it such that only those satisfying T_j can decrypt so that,

$$C_j = Enc_{T_j}(res_j) \tag{2}$$

- Decryption Condition: A user u_i can decrypt the ciphertext C_j (representing resource res_j) if and only if their attribute set Ai satisfies the access tree policy T_j. This is denoted by the satisfiability relation $A_i \models T_j$.

This ABE mechanism ensures that even if a user somehow gains unauthorized access to an encrypted resource (e.g., through a compromised cloud storage), they cannot make sense of its content unless their personal attributes match the resource's predefined access policy.

3.4 Data Transmission & Integrity Verification

Maintaining the integrity and authenticity of data during transmission across the cloud network is paramount. This model incorporates cryptographic hashing and digital signatures.

- Original Data (D): The data intended for transmission.
- Cryptographic Hash $(H(D))$: A fixed-size unique fingerprint of the data, computed using a secure hash function (e.g., SHA-256). Any alteration to the data will result in a different hash.
- Digital Signature (S): The sender computes a hash of the data $H(D)$ and then encrypts this hash using their private key. This creates a digital signature $S = Sign_{priv}(H(D))$. The signature provides authentication (proof of sender's identity) and non-repudiation (sender cannot deny having sent the data).
- Verification: Upon receiving the transmitted data D', the receiver computes its hash $H(D')$. The receiver then uses the sender's public key to decrypt the received digital signature S. If the decrypted signature matches $H(D')$, the data's integrity is verified (it hasn't been altered), and the sender's authenticity is confirmed so that,

$$Verify_{pub}(S, H(D')) = True \tag{3}$$

This mechanism guarantees that resources exchanged within the digital music classroom remain untampered and originate from legitimate sources.

3.5 Secure Session Establishment (TLS-Like)

All communications between clients (e.g., students' devices) and the cloud server are secured using a TLS-like protocol, ensuring confidentiality and integrity of data in transit.

- Shared Session Key (K_s): A unique, ephemeral symmetric session key K_s is securely generated and exchanged during a handshake phase (e.g., using Diffie-Hellman or ECDH key exchange). This key is valid only for the current session, providing Perfect Forward Secrecy.
- Symmetric Encryption/Decryption: All messages m exchanged during the session are encrypted using this shared session key $(E_{K_s}(m))$ by the sender and decrypted by the receiver $(D_{K_s}(m'))$ i.e. $m' = E_{K_s}(m)$ and $m = D_{K_s}(m')$

This ensures that all live sessions, file transfers, and other communications remain confidential and protected from eavesdropping and tampering by unauthorized third parties.

3.6 Anomaly-Based Intrusion Detection (Behavioral Monitoring)

An additional component of the NS-CDMC model is a dynamic anomaly detection system, which keeps tabs on user actions in order to spot questionable ones. A feature vector $x(t) \in \mathbb{R}^d$ is created at regular intervals to describe the user's current activity pattern. Some of the metrics that could be included in this vector are the frequency of login attempts, the methods used to access resources, the times of day when these attempts are made, and the amount of bandwidth used.

- Normal Behavior Profile (μ, Σ): The system develops a statistical profile of "normal" user activity, which is usually shown by a mean vector μ and a covariance matrix Σ that come from past lawful actions.
- Mahalanobis Distance $(D_M(x))$: This metric looks at the correlations between various aspects to see how similar a fresh observation x is to the taught normal profile. A larger Mahalanobis distance means that behavior is more different from what is usual and is written as,

$$D_M(x) = (x - \mu)^T \Sigma^{-1} (x - \mu) \tag{4}$$

- Anomaly Classification: If the Mahalanobis Distance for a certain activity vector x is greater than a set threshold δ, the activity is considered an anomaly, which might indicate that someone is trying to break in or use the system inappropriately.

$$Anomaly(x) = \begin{cases} 1 & if\ D_M(x) > \delta \\ 0 & otherwise \end{cases} \tag{5}$$

Mahalanobis distance is a statistical measure that evaluates the distance of a point from the mean of a distribution, taking into account the

correlations between variables. This makes it effective for detecting anomalies in multivariate data. Unlike Euclidean distance, Mahalanobis distance considers the covariance structure of the data, making it more sensitive to anomalies that deviate from expected patterns considering the relationships between variables. In contexts like user behavior analysis where multiple features (like login times, access patterns, etc.) are considered, Mahalanobis distance can effectively identify unusual patterns.

3.7 Audit Logging and Accountability

For accountability, forensic analysis, and compliance, audit logging must be complete and show signs of tampering.

- Log of Access Events (L): Every significant action within the system, especially access attempts and decisions, is recorded as an event log. Each log entry is a tuple (u, p, res, t) where, u is the ID of the user performing the action, p denotes operation or permission requested/performed, res is target resource of the operation and t is precise timestamp of the event.
- Tamper-Evident Logs (Hash Chains): Cryptographic hash chains connect the audit logs together to make sure they are safe and can't be changed. Each new log entry log_i is hashed along with the hash of the previous log entry $h_i - 1$ to produce the new hash h_i i.e.

$$h_i = H(h_i - 1 \parallel log_i) \tag{6}$$

The symbol $\parallel$ denotes concatenation. This chaining makes it computationally infeasible to alter any past log entry without invalidating all subsequent hashes, thereby immediately revealing any tampering attempts.

Figure 3 presents the framework for the proposed model.

Algorithm 1: NS-CDMC Security Framework Operation
Input: User Request (u, res, p) (User u requests operation p on resource res)

Output: Access Decision (Permit/Deny) and System Security Actions
System Components Initialization:

- Initialize User Set U, Role Set R, Permission Set P, Resource Set RES.
- Define assign function (User-to-Role mapping) and perm function (Role-to-Permission mapping).

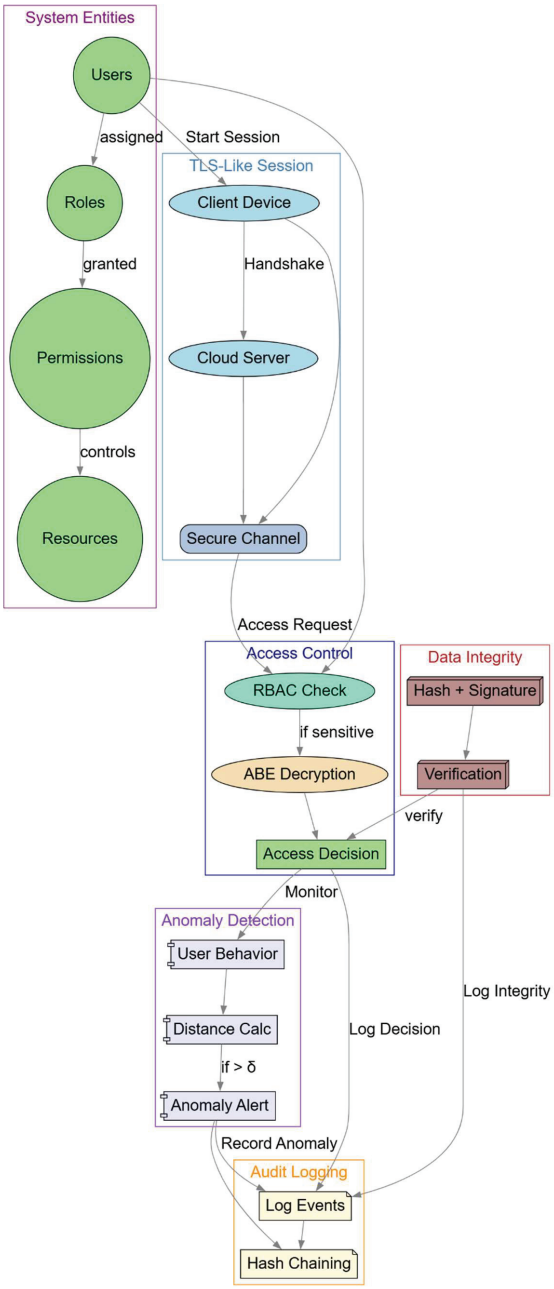

Figure 3 The framework for the proposed model.

- Initialize User Attribute Set A, and define Access Tree Policies T_j for each sensitive resource res_j.
- Initialize Secure Hash Function $H(\cdot)$, Private Key $priv$, Public Key pub.
- Initialize Anomaly Detection Model (Mahalanobis Distance parameters μ, Σ, and threshold δ).
- Initialize Audit Log L with initial hash h_0.

Procedure:

1. **Secure Session Establishment (TLS-Like):**
    - Action: When User u initiates communication with the Cloud Server.
    - Step 1.1 (Handshake): Client and Server perform a TLS-like handshake (e.g., using ECDH).
    - Step 1.2 (Key Generation): Securely negotiate a shared ephemeral symmetric session key K_s.
    - Step 1.3 (Mutual Authentication): (Optional but Recommended) Both client and server authenticate each other using digital certificates.
    - Output: Encrypted communication channel established using K_s.
    - Log: Record session establishment details in Audit Log.
2. **Resource Access Request Processing:**
    - Input: User request (u, res_j, p_k) arrives at the Cloud Server via the secure TLS session.
    - Step 2.1 (RBAC Access Control):
        - Check: Verify if user u is permitted to perform operation pk on resource res_j based on RBAC rules.
        - Condition: $\exists r \in assign(u)$ such that $(p_k, res_j) \in perm(r)$.
        - If Condition False:
            - Action: Deny access.
            - Log: Record "Access Denied (RBAC)" for (u, p_k, res_j) in Audit Log.
            - Return: Deny.
    - Step 2.2 (ABE Fine-Grained Control - for Encrypted Resources):
        - Check: If res_j is a sensitive resource requiring ABE decryption.
        - Condition: User's attribute set A_u satisfies the resource's access tree policy T_j ($A_u \models T_j$).

- If Condition False (and resource is ABE encrypted):
  - Action: Deny access (cannot decrypt).
  - Log: Record "Access Denied (ABE)" for (u, p_k, res_j) in Audit Log.
  - Return: Deny.

- Step 2.3 (Perform Permitted Operation and Data Integrity):
  - If RBAC and ABE (if applicable) Permit:
    - Action (Data Transmission - Read/Download):
      - Retrieve resource res_j.
      - Compute hash $H(res_j)$.
      - Retrieve original stored hash h_j for res_j.
      - Verification: If $H(res_j) \neq h_j$:
        - Action: Flag data corruption, do not transmit, log "Integrity Breach".
        - Return: Deny.
      - Transmit: If integrity OK, transmit res_j (or its decrypted form if ABE was applied) to u via the secure TLS session, with sender's digital signature $S = Sign_{priv}(H(res_j))$.
      - Receiver Verification: On client side, $Verify_{pub}(S, H(resj')) = True$.
    - Action (Data Transmission - Write/Upload/Edit):
      - Receive data D' from u via the secure TLS session.
      - Verification: Verify digital signature of D' using $Verify_{pub}(S, H(D')) = True$. If verification fails, flag integrity/authenticity issue.
      - Store/Update: If integrity/authenticity OK, store or update res_j with D'.
      - Update Hash: Compute and store new hash $h_j = H(res_j)$.
    - Output: Access Permitted.
    - Log: Record "Access Permitted" for (u, p_k, res_j) in Audit Log.

3. **Anomaly-Based Intrusion Detection (Behavioral Monitoring):**
   - Trigger: Periodically or upon each user action.

- Step 3.1 (Feature Vector Generation): For the current user u's activity at time t, construct feature vector $x(t) \in \mathbb{R}^d$. This includes metrics like:
  - Login frequency, resource access patterns, time of day.
  - Number of failed login/access attempts.
  - Bandwidth usage.
  - Sequence of operations.
- Step 3.2 (Anomaly Scoring): Calculate Mahalanobis Distance $D_M(x(t))$ for x(t) relative to the learned normal behavior profile (μ, Σ).

$$D_M(x) = (x - \mu)^T \Sigma^{-1} (x - \mu)$$

- Step 3.3 (Anomaly Classification):
  - Condition: If $D_M(x(t)) > \delta$ (predefined threshold).
  - If Condition True:
    - Action: Classify as Anomaly (return 1).
    - Alert: Generate security alert to administrator.
    - Response: Initiate predefined response (e.g., temporary suspension of user session, detailed logging).
    - Log: Record "Anomaly Detected" details, including contributing features from x(t) if XAI is integrated.
  - If Condition False:
    - Action: Classify as Normal (return 0).

4. **Audit Logging and Accountability:**
   - Trigger: After every significant system event (e.g., login, access request, access decision, file transfer, anomaly detection).
   - Step 4.1 (Log Entry Creation): Create a log entry $log_i = (u, p, res, t, decision, anomaly_{status}, timestamp)$.
   - Step 4.2 (Hash Chaining): Compute the new hash h_i by concatenating the previous log hash $h_i - 1$ with the current log entry log_i, and then hashing the result.

$$h_i = H(h_i - 1 \parallel log_i)$$

   - Step 4.3 (Storage): Append (log_i, h_i) to the Audit Log L.
   - Step 4.4 (Integrity Verification): Periodically verify the integrity of the entire log chain by re-computing hashes and comparing them from h_0 to h_N.

A strong, multi-layered security system is made possible by the way Role-Based Access Control (RBAC) and Attribute-Based Encryption (ABE) work together. RBAC is a broad administrative access control layer, whereas ABE is a more specific data-level encryption layer. Together, they make sure that access is handled in a systematic way and that data is safeguarded at the encryption level according on the user's individual qualities.

- RBAC as the First Gatekeeper: RBAC is the main way to regulate access. The system initially verifies the RBAC permissions when a user asks to do anything with a resource, such "view" a file. It checks to see whether the user has authorization to access the resource via their allocated role. If the user's role-based permissions don't allow the desired action, access is refused right away, and the ABE layer is never used.
- ABE as the Second Layer of Defense: If the RBAC check succeeds, which means the user's role grants them broad authority to access the resource, the system continues on to the ABE layer. This layer is in charge of decrypting the resource. The resource is encrypted with an ABE policy (an "access tree") that only lets certain people in depending on certain criteria (for example, "department = finance" AND "security_level = high").
- Attribute Matching for Decryption: The system compares the user's characteristics to the ABE policy that is built into the encrypted resource. The user gets the cryptographic key they need to decrypt and see the data if their characteristics meet the policy's requirements. Even if the RBAC layer allowed them "access," they can't decrypt the file if their characteristics don't fit the policy.

4 Experimental Setup

The experimental setup simulates a cloud-based digital music classroom with real-world complexity, comprising 40 virtual machines, including 20 student clients, 5 instructors, 5 admin/TA accounts, and 5 cloud music servers. The network architecture includes an internal LAN for student-instructor access, a secure VLAN for instructor/admin operations, and an edge gateway for internet/stream access. The simulation also includes 5 malicious/anomalous nodes for attack simulation, with intrusion vectors such as insider abuse, account compromise, and anomalous playback/download behavior. The dataset consists of user actions, including play, upload, download, view, and login activities, as well as system logs from Linux, Windows, and API Gateway. The dataset also includes injected anomalies based on NSL-KDD [https:

//www.kaggle.com/datasets/hassan06/nslkdd] and UNSW-NB15 dataset [https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15], simulating real-world attack scenarios. A custom log generator simulates streaming, access violations, and burst anomalies, providing a comprehensive dataset for evaluating the NS-CDMC model.

4.1 Simulation Variables and Hyperparameters

The software tools used in the simulation include VMware ESXi and VirtualBox for virtualization, and Windows 10 for operating systems, and OpenABE, PyCrypto, and OpenSSL for security libraries. Python 3.9 + SimPy are used to build the behavior simulator, while NumPy is used to analyze the data. TensorFlow is used to model trust, while a custom Mahalanobis engine and PyOD are used to find anomalies. The simulation includes users (U), role types (R), resources (RES), permissions (P), trust scores (τ), and Mahalanobis distance (D_M) for anomaly detection. Simulation variables for access control decision latency ($T_{latency}$) and anomaly labels (A) are supplied. These criteria measure NS-CDMC model problem recognition and access management. The hyperparameters of the NS-CDMC model are the initial trust score (τ_0), positive reinforcement factor (α), negative penalty (β), trust decay factor (γ), and Mahalanobis threshold (θ_M) ABE layer policy depth is 3-4 layers using ABE encryption. Decision engine access latency must be less than 50 ms, and the simulator must run for three hours each session across 10 sessions. We evaluate the NS-CDMC model using many criteria. Access control decision delay, false positive rate, trust drift, privilege revocation, and system throughput are examples. These findings show the model can detect issues, limit access, and maintain system performance.

4.2 Experimental Design

Each simulation captures access choices, trust score changes, anomaly scores, and ABE policy applications. Starting points include RBAC-only, ABE with static rules, machine-learning anomaly detection, and hybrid statistical monitoring. The simulation results are used to assess the NS-CDMC model and compare it to other methods.

4.3 Security Mechanism for Digital Music Classrooms

Many components make up the NS-CDMC security framework (Figure 4), which provides a secure, real-time, and user-friendly environment. The user's

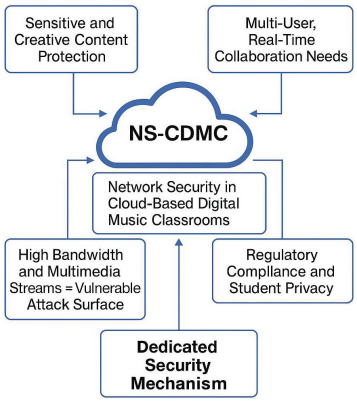

Figure 4 NS-CDMC dedicated security mechanism.

attributes are used to encrypt private data via attribute-dependent encryption (ABE). This guarantees that only authorized users may see particular content. Based on trust, RBAC and TBAR dynamically change access control. This offers contextually appropriate and adaptable permissions. However, Anomaly Detection analyzes user activity and notifies them to abnormalities. This helps detect business and external security risks. Finally, the system's low False Positive Rate (FPR) ensures smooth digital communication without unwanted alerts, giving consumers a secure and seamless experience. These components form NS-CDMC, a secure system that protects sensitive data and allows real-time collaboration.

4.3.1 Sensitive and creative content protection

Student compositions, performances, and projects, licensed or copyrighted audio and video files, and proprietary teaching materials are used in digital music schools. Without permission, obtaining or leaking this material may be intellectual property theft, copying, or licensing violation. This may impact schools, instructors, and students. NS-CDMC uses Attribute-According Encryption to reduce risk. This restricts material decoding to registered students and instructors based on their positions, courses, and instruments. This method is practical and flexible for protecting sensitive and creative resources in digital music schools.

Attribute-Based Encryption (ABE) successfully hides sensitive and creative digital content, as seen in Figure 5. ABE preserves digital rights, prohibits copying, and enforces licensing agreements by restricting digital information access. Due to their function, course, or instrument, only certain

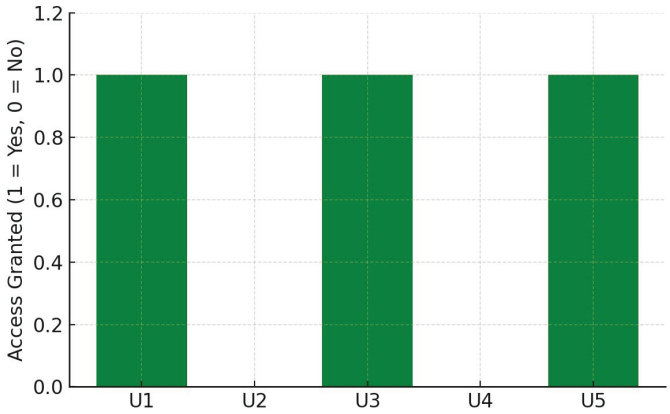

Figure 5 ABE access based on attributes.

individuals may view particular content, according to the story. Green bars indicate this. Red bars indicate that non-qualifiers are denied access. This limited access technique preserves digital rights and follows material protection laws. From this narrative, we may learn that ABE restricts access to particular materials, enforces content protection laws, and defends digital rights.

4.3.2 Multi-user, real-time collaboration needs

Digital music classes often include live jam sessions, teacher commentary on compositions, and group performance evaluations. All of them need real-time, ever-changing collaboration from many people. Because they cannot adapt to user roles, permissions, or situations, username-password systems and other standard access control methods fail in collaborative settings. RBAC and TBAR are used in the NS-CDMC paradigm to solve this challenge. This lets permissions adjust based on system usage or class participation. This technology allows large-scale collaboration in digital music schools secure and straightforward.

Trust-depending Access Refinement (TBAR) changes user access in real time based on system trust (Figure 6). Access control models may alter depending on user behavior using TBAR. This paradigm is behavior-based and dynamic. Digital music lessons and other real-time collaborative situations benefit from this. The person's behavior determines their trust score, which signals access. Users with trust scores over 0.6 have higher privileges. They may edit, upload, or conduct sessions. This method bases rights on trustworthiness. This is context-aware permissions. The most essential lessons

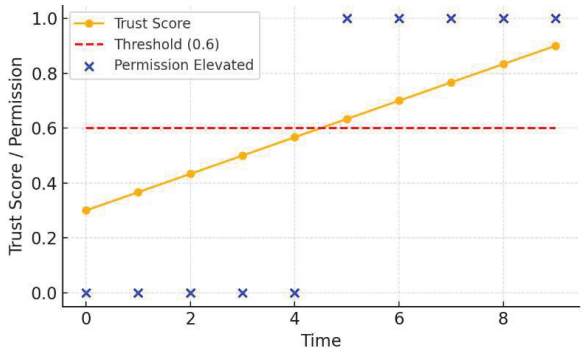

Figure 6 Trust-based permission elevation.

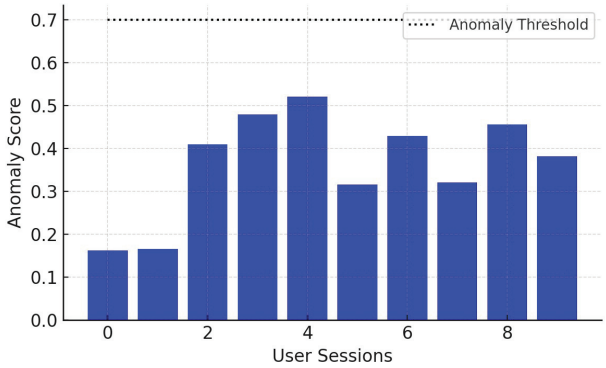

Figure 7 Anomaly-based intrusion detection.

from this plot are that confidence increases rights, the dynamic access model changes with behavior, and TBAR makes permissions scenario-based.

4.3.3 Behavior-driven threats (internal and external)

Digital music classrooms face internal and external behavioral hazards. Students may exchange passwords, bypass security, or misuse other students' resources. These unique behaviors may bypass password-only limitations. Data misuse or grade manipulation may result. NS-CDMC uses machine learning to identify anomalous user activities such checking in at odd times, downloading excessively, or pretending to be somewhere else. The issue is resolved. Identifying and resolving security issues before they happen keeps digital music schools secure.

Figure 7 displays the NS-CDMC system's anomaly-based intrusion detection's effectiveness. It flags anomalous conduct based on users'

behavioral deviation ratings. The application looks for outliers using a predefined anomalous threshold (such as 0.7). Red bars highlight security risks. People that do their jobs properly get blue bars. This detection system may detect internal hazards like students abusing the system and external threats like illegal access. More proactive than barring access, Anomaly-Based Intrusion Detection protects your PC. Detecting odd behavior lets you react to security problems promptly. This picture depicts how anomaly detection may identify unexpected behavior, how red bars reflect weirdly behaved individuals, and how the detection strategy adds safety to standard access limits.

4.3.4 False alarms are disruptive in real-time classrooms

Digital music course streaming must be uninterrupted. False alerts or limited access may make studying, canceling live performances, and postponing feedback sessions difficult. The NS-CDMC model has a 0.03 False Positive Rate, suggesting less unnecessary interruptions than other IDS models. This method keeps digital music classes running smoothly and securely without interruption. This improves professor and student study.

Figure 8 highlights the system's accuracy and dependability, focusing on the False Positive Rate. The FPR is 0.03 (3%), and the system seldom malfunctions. This is essential for live music and system usability. This shows that the NS-CDMC system is simple and balances speed and accuracy, reducing security threats. The best parts of this performance are that it permits continuous live music sessions, balances speed and precision, and is simple

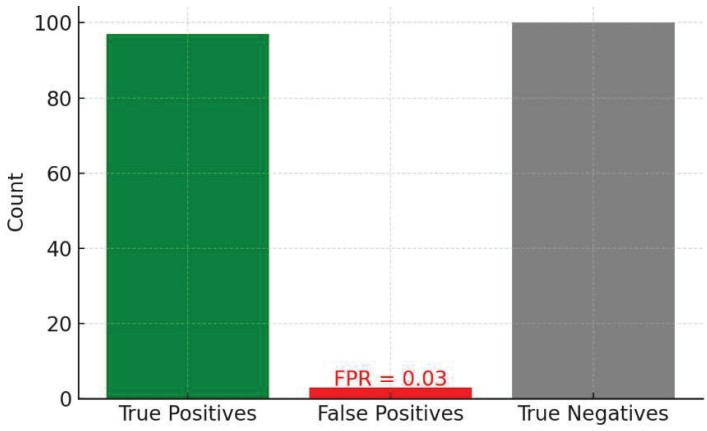

Figure 8 False positive rate (FPR) visualization.

to use without compromising security. Customers have a safe and seamless experience.

5 Results and Discussion

This paper illustrates the superior performance of the NS-CDMC model across critical security metrics when compared to several benchmark methods [21–24]. The results focus on a specific performance indicator, demonstrating the advantages stemming from NS-CDMC's integrated and intelligent design.

The NS-CDMC model's Dynamic Trust-depending Access Refinement (TBAR) layer is presented in Figure 9. It demonstrates how user behavior affects trust score over time. The x-axis represents user activity times, while the y-axis shows the normalized trust score, which runs from 0 to 1. The blue line reflects the user's trust score over time. It begins high and fluctuates erratically throughout normal exercise. Trust drops substantially when someone does something bad. This implies increased access permissions are revoked when the score drops below specific standards. Access to basic resources, uploading files, and downloading files is limited. Trust increases when negative behavior decreases. When the score reaches the access level threshold, permissions gradually return. Based on security situation and user behavior, NS-CDMC's adaptive security adjusts access in real time. Security is more adaptable than static access control. The new TBAR layer may

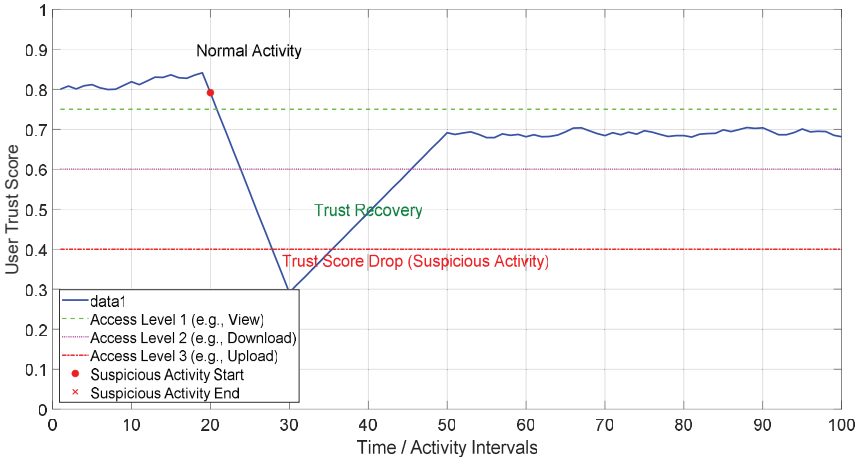

Figure 9 Dynamic trust-based access refinement using NS-CDMC.

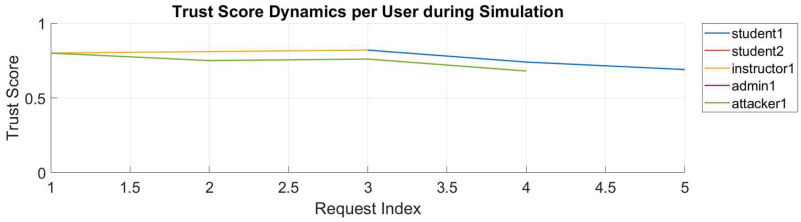

Figure 10 Trust score dynamics per user during simulation.

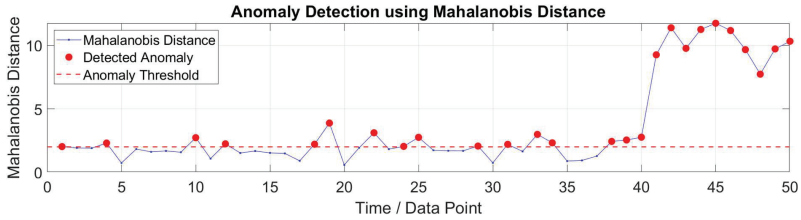

Figure 11 Anomaly detection using Mahalanobis distance.

change access depending on behavior. This reduces account breaches and insider assaults, improving security. User rights are easier to handle with dynamic response than RBAC or ABE models.

The NS-CDMC model's Trust-depending Access Refinement is shown in Figure 10. System assessments and simulated behaviors affect user trust ratings. The x-axis shows the access request sequence, while the y-axis shows each user's 0–1 trust rating. Users' trust scores grow along the colored lines. Positive incentives for good behavior and negative repercussions for refused requests effect the score. The graphic shows adaptive security, which adjusts to user behavior. It's more secure than static permissions. The attacker's trust score plummets owing to suspicion. Rights or attention may be lost. The TBAR component constantly adapts to strengthen and optimize the NS-CDMC model's security.

Figure 11 shows how the Anomaly-Based Intrusion Detection System, which is an important part of NS-CDMC, works. It shows the difference between normal and abnormal user activity patterns by calculating their Mahalanobis distance from a learnt profile of typical behavior. The x-axis depicts a series of observations of how users behave, and the y-axis shows the Mahalanobis distance, which is a statistical measure of how far apart from typical behavior someone is. The blue line shows the Mahalanobis distance that was computed for each data point. Most of the points are in a

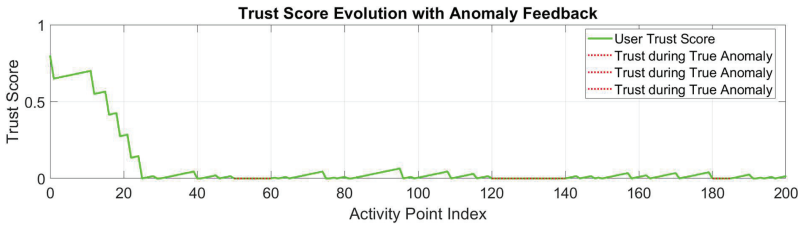

Figure 12 Trust score evolution with anomaly feedback.

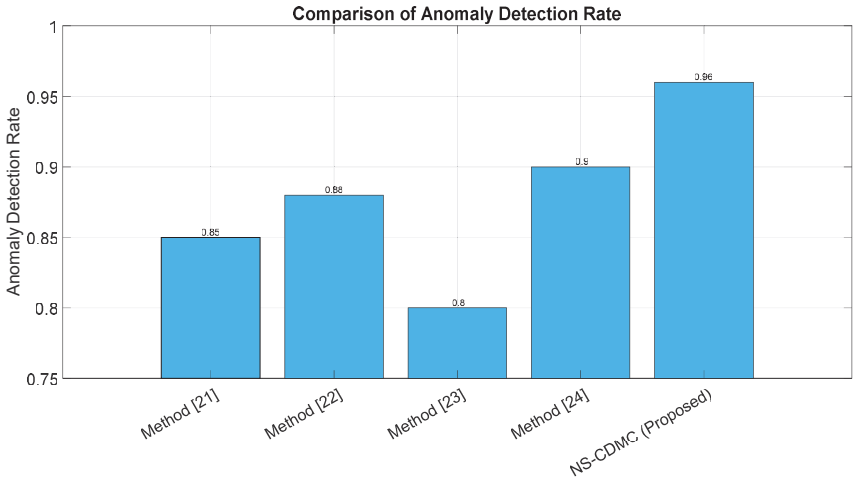

Figure 13 Comparison of anomaly detection rate.

lower range, which means they are consistent with typical behavior. The red dashed line shows the anomaly threshold. Data points that go over this line are called anomalies and are highlighted with red circles. The figure shows how well the algorithm can find strange patterns, even when they are put there on purpose. This ability to find anomalies adds an extra layer of protection against insider threats, hacked accounts, or new attack methods, in addition to classic security measures like RBAC and ABE. By keeping an eye on how people behave, NS-CDMC makes its security stronger so that it can find and deal with any security problems or abuse.

Figure 12 extends the anomaly detection from the previous general example. It generates a longer sequence of user activities, identifies anomalies using Mahalanobis distance, and then directly feeds back the anomaly detection result into the user's trust score.

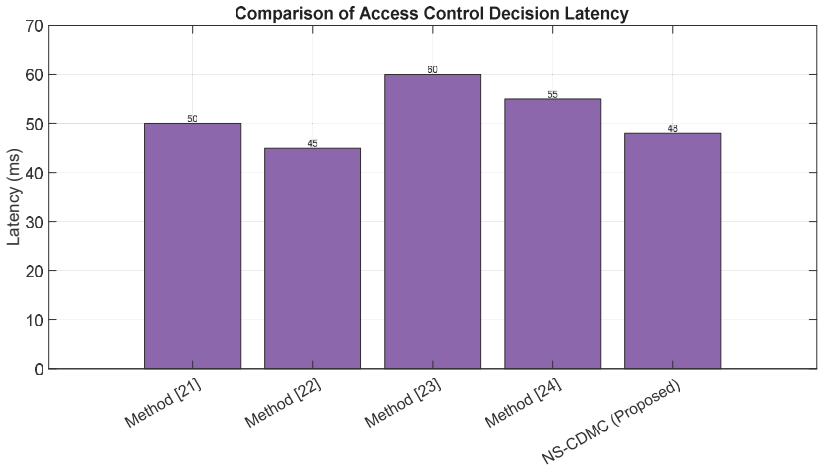

Figure 14 Comparison of access control decision latency.

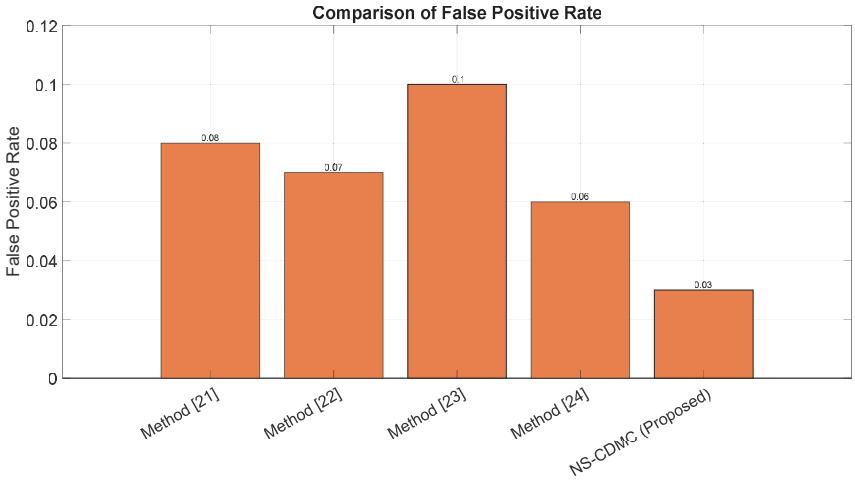

Figure 15 Comparison of false positive rate.

The Anomaly Detection Rate (ADR) comparison plot (Figure 13) demonstrates the effectiveness of the proposed NS-CDMC method in identifying anomalous activities. The x-axis lists the benchmark methods and NS-CDMC, while the y-axis represents the percentage of actual anomalies correctly identified. The plot shows that NS-CDMC outperforms other methods with a significantly higher ADR of 0.96, indicating its ability to detect sophisticated threats and insider misuse. This superior performance is attributed to

NS-CDMC's integrated behavioral monitoring using Mahalanobis Distance, which analyzes subtle deviations in user activity patterns.

In Figure 14, the Access Control Decision Latency comparison plot, the suggested NS-CDMC technique handles access requests effectively. The x-axis shows benchmark approaches and NS-CDMC, while the y-axis shows decision time. The chart shows that NS-CDMC's 48 ms latency is similar to or lower than other benchmark techniques. NS-CDMC's design allows efficient processing despite extra security levels. This may be due to better algorithms, parallel computing, or early leave. This proves that security doesn't necessarily hurt performance, making NS-CDMC ideal for real-time cloud systems.

The False Positive Rate (FPR) comparison plot (Figure 15) illustrates how effectively the NS-CDMC strategy reduces false alarms. The x-axis displays benchmark approaches and NS-CDMC, while the y-axis shows the percentage of routine activities wrongly designated as anomalies. Figure shows that NS-CDMC has a substantially lower FPR of 0.03 than other methods. This allows it to distinguish between malicious and legitimate abnormalities. NS-CDMC employs many security layers, including RBAC, ABE, TBAR, and behavioral monitoring, to reduce false alerts and improve operations.

6 Conclusion and Future Work

This research presented NS-CDMC, a smart network security paradigm for Cloud-Based Digital Music Classrooms. Using RBAC, ABE, dynamic trust-based access refinement (TBAR), strong data integrity verification, secure session establishment, and a complex anomaly-based intrusion detection system, NS-CDMC solves cloud-based educational environment security issues. Experiments reveal that the NS-CDMC model performs well. NS-CDMC had a relatively high ADR of 0.96 in our comparative research. It finds complicated and nuanced harmful activities better than benchmark techniques. For practical application, NS-CDMC showed a low False Positive Rate (FPR) of 0.03. This minimized false alarm work. NS-CDMC's average access control decision latency was 48ms, proving that security doesn't always imply poor performance. Real-time user behavior adaptation via the TBAR component is a major improvement over static security solutions. It reduces insider assaults and compromised accounts continuously. The model's defenses against new attack vectors are strengthened by proactive Mahalanobis distance anomaly detection. We conclude that the NS-CDMC model's robust, flexible, and high-performance security architecture dramatically enhances digital music

classroom contents and user interactions. Due to its integrated design and improved anomaly detection and false positive reduction, NS-CDMC is a viable solution to safeguard cloud-based educational platforms from shifting cyber threats.

Future work should focus on making the present hybrid data protection system for digital music schools more secure, scalable, and user-friendly. There are a few important topics that this covers. First, it is important for digital music classrooms to be able to work with cloud and IoT devices so that they can serve a larger variety of platforms. This means that new Attribute-Based Encryption (ABE) standards are needed for these contexts. Second, dynamic policy updates and revocation would let user access privileges alter in real time depending on changes in role or characteristics. This would be safe since it would include a strong revocation mechanism. Third, a full performance and scalability test is required to see how latency, computational overhead, and scalability change when more people and resources are added. Fourth, creating a user-friendly interface and policy management system would make it easier to manage roles, permissions, and ABE rules using a graphical interface. Finally, integrating blockchain might make security and trust better by making a permanent record of access control choices for compliance and audit purposes.

Acknowledgments

The research is supported by Project from the Third Batch of Henan Province First-class Undergraduate Courses “Music and Aesthetice: Practice and Communication” (jiaogao [2022] No. 324); Interim Result of the First Batch of University-level Intelligent Curriculum Program “Music Appreciation”.

References

[1] P. Gupta, R. Mahajan, U. Badhera, P.S. Kushwaha, Integrating generative AI in management education: a mixed-methods study using social construction of technology theory, Int. J. Manag. Educ., 22(3) (2024), Article 101017.

[2] Chen, Z. 2024. Campus Network Security Intrusion Detection Based on Feature Segmentation and Deep Learning. Journal of Cyber Security and Mobility. 13, 04 (Jun. 2024), 775–802. https://doi.org/10.13052/jcsm2245-1439.1349.

[3] E. Balamurugan, A. Mehbodniya, E. Kariri, K. Yadav, A. Kumar, M. Anul Haq, Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN), Pattern Recognit. Lett., 156 (2022), pp. 142–151.
[4] M. Wang, Optimization of network security in university laboratories based on anomaly intrusion detection in public cloud networks Comput. Electr. Eng., 111 (2023), Article 108968.
[5] N. Basil, H.M. Marhoon, Selection and evaluation of FOPID criteria for the X-15 adaptive flight control system (AFCS) via Lyapunov candidates: optimizing trade-offs and critical values using optimization algorithms, e Prime Adv. Electr. Eng. Electron. Energy, 8 (2024), article 100589.
[6] N. Basil, H.M. Marhoon, A.F. Mohammed, Evaluation of a 3-DOF helicopter dynamic control model using FOPID controller-based three optimization algorithms, Int. J. Inf. Technol. (2024), pp. 1–10.
[7] N. Basil, B.M. Sabbar, H.M. Marhoon, A.F. Mohammed, A. Ma'arif, Systematic review of unmanned aerial vehicles control: challenges, solutions, and meta-heuristic optimization, Int. J. Robot. Control Syst., 4(4) (2024).
[8] L.C. Costa, et al., OpenFlow data planes performance evaluation, Perform. Eval., 147 (2021), Article 102194.
[9] A.R. Ibrahim, N. Basil, M.I. Mahdi, Implementation enhancement of AVR control system within optimization techniques, Int. J. Nonlinear Anal. Appl., 12(2) (2021).
[10] H.M. Marhoon, N. Basil, A. Ma'arif, Exploring blockchain data analysis and its communications architecture: achievements, challenges, and future directions: a review article, Int. J. Robot. Control Syst., 3(3) (2023), pp. 609–626.
[11] H.M. Marhoon, N. Basil, A.F. Mohammed, Medical Defense Nanorobots (MDNRs): a new evaluation and selection of controller criteria for improved disease diagnosis and patient safety using NARMA (L2)-FOP+ D (ANFIS) μ–Iλ-based Archimedes Optimization Algorithm, Int. J. Inf. Technol. (2024), pp. 1–11.
[12] M. Erel-Özçevik, Sustainable fixed wireless access with blockchain secured software defined network, Pervasive Mob. Comput., 92 (2023), Article 101803.

[13] N. Indrason, G. Saha, Exploring Blockchain-driven security in SDN-based IoT networks, J. Netw. Comput. Appl., 224 (2024), Article 103838.

[14] R. Iqbal, R. Hussain, S. Arif, N.M. Ansari, T.A. Shaikh, Data analysis of network parameters for secure implementations of SDN-based firewall, Comput. Mater. Contin., 77(2) (2023), pp. 1575–1598.

[15] Debnath S, Ganguly N, Mitra P (2008) Feature weighting in content based recommendation system using social network analysis[C]//Proceedings of the 17th international conference on World Wide Web. 1041–1042.

[16] Bagul DV, Barve S (2021) A novel content-based recommendation approach based on LDA topic modeling for literature recommendation[C]//2021 6th International conference on inventive computation technologies (ICICT). IEEE: 954–961.

[17] He X, Liao L, Zhang H et al. (2017) Neural collaborative filtering[C]//Proceedings of the 26th international conference on world wide web. 173–182.

[18] Chen T, He X, Kan MY (2016) Context-aware image tweet modelling and recommendation. Proceedings of the 24th ACM international conference on Multimedia, pp. 1018–1027. https://doi.org/10.1145/2964284.2964291.

[19] Selmene S, Kodia Z (2020) Recommender System Based on User's Tweets Sentiment Analysis. Proceedings of the 4th International Conference on E-Commerce, E-Business and E-Government, pp. 96–102. https://doi.org/10.1145/3409929.3414744.

[20] Sánchez-Moreno D, Zheng Y, Moreno-García MN (2018) Incorporating time dynamics and implicit feedback into music recommender systems. Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, pp. 580–585. https://doi.org/10.1109/WI.2018.00-34.

[21] Kayes, A.S.M.; Kalaria, R.; Sarker, I.H.; Islam, M.S.; Watters, P.A.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues. *Sensors* **2020**, *20*, 2464. https://doi.org/10.3390/s20092464.

[22] L. Zhang, H. Li, Y. Zhang and F. Khan, "Efficient privacy-preserving decentralized ABE supporting expressive access structures," *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Atlanta, GA, USA, 2017, pp. 547–552, doi: 10.1109/INFCOMW.2017.8116436.

[23] Schummer, P.; del Rio, A.; Serrano, J.; Jimenez, D.; Sánchez, G.; Llorente, Á. Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation. *AI* **2024**, *5*, 2967–2983. https://doi.org/10.3390/ai5040143.

[24] Ogwara, N.O.; Petrova, K.; Yang, M.L.; MacDonell, S.G. MINDPRES: A Hybrid Prototype System for Comprehensive Data Protection in the User Layer of the Mobile Cloud. *Sensors* **2025**, *25*, 670. https://doi.org/10.3390/s25030670.

[25] Fan W, Derr T, Ma Y et al. (2019) Deep adversarial social recommendation. arXiv preprint arXiv:1905.13160.

[26] Zheng E, Kondo GY, Zilora S et al. (2018) Tag-aware dynamic music recommendation. Expert Syst Appl 106:244–251

[27] Hu Y, Koren Y, Volinsky C (2008) Collaborative filtering for implicit feedback datasets[C]//2008 Eighth IEEE international conference on data mining. IEEE 15:263–272.

[28] Liu CL, Chen YC (2018) Background music recommendation based on latent factors and moods. Knowl Based Syst 159:158–170.

[29] Li T, Choi M, Fu K et al. (2019) Music sequence prediction with mixture hidden markov models[C]//2019 IEEE International Conference on Big Data (Big Data). IEEE: 6128–6132.

[30] Flexer A, Stevens J (2018) Mutual proximity graphs for improved reachability in music recommendation. J new Music Res 47(1):17–28.

[31] Choi S, Ha H, Hwang U et al. (2018) Reinforcement learning based recommender system using biclustering technique. arXiv preprint arXiv:1801.05532

Biography

Lina Song, female, Han ethnicity, born in 1983, is a member of the Communist Party of China and an associate professor. She has been recognized as an Academic and Technical Leader by the Henan Provincial Department of Education and a Young Backbone Teacher in Henan Higher Education Institutions. She has led key teaching reform research and practice projects in higher education in Henan Province and is responsible for a provincial-level first-class undergraduate course. Additionally, she was awarded the Second Prize in Higher Education Teaching Achievements by Henan Province. She has published over 20 academic papers and authored four monographs and textbooks. She has presided over nearly 20 research projects at the provincial and departmental levels, five of which received first-class awards. Currently, she serves as the Director of the Public Art Education Center at Zhongyuan Institute of Science and Technology.