Cyber Neutrosophic Model for Secure and Uncertainty Aware Evaluation in Indoor Design Projects

[1]Manju A, [2]Rukmani Devi S, [3]Mohammed Alaa H Altemimi, [4]Jwalant Baria, [5]Arivazhagan D and [6]Lakshmi Prasanna P

[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.

[2]Department of Computer Science and Engineering, Saveetha College of Liberal Arts and Sciences, SIMATS Deemed to be University, Saveetha Nagar, Thandalam, Chennai, Tamil Nadu, India.

[3]Department of Information and Communication Engineering, Al-Khwarizmi College of Engineering, The University of Baghdad, Baghdad, 10071, Iraq.

[4]Department of Computer Science and Engineering, Government Engineering College Dahod, Dahod, Gujarat, India.

[5]AMET Business School, Academy of Maritime Education and Training Deemed to be University, Chennai, Tamil Nadu, India.

[6]Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.

[1]manjuappukuttan1985@gmail.com, [2]rukmanibaveshnambi@gmail.com, [3]mohammed.alaa@kecbu.uobaghdad.edu.iq, [4]jwalant.baria@gmail.com, [5]prof.arivazhagan@ametuniv.ac.in, [6]lakshmiprasannap87@gmail.com

Correspondence should be addressed to Manju A : manjuappukuttan1985@gmail.com

Article Info

Journal of Machine and Computing (https://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202505140
Received 12 January 2025; Revised from 29 April 2025; Accepted 16 June 2025.
Available online 05 July 2025.

Abstract – To perform a secure evaluation of Indoor Design data, the research introduces a Cyber-Neutrosophic Model, which utilizes AES-256 encryption, Role-Based Access Control, and real-time anomaly detection. It measures the percentage of unpredictability, insecurity, and variance present within model features. Also, it provides reliable data security. Similar features have been identified between the final results of the study, corresponding to the Cyber-Neutrosophic Model analysis, and the cybersecurity layer helped mitigate attacks. It is worth noting that Anomaly Detection successfully achieved response times of less than 2.5 seconds, demonstrating that the model can maintain its integrity while providing privacy. Using neutrosophic similarity scores that ranged from 0.85 to 0.98, the Cyber-Neutrosophic Model proved to have higher analysis accuracy. Additionally, it provided robust data security by utilizing Advance Encryption Standards (AES)-256 with Role-Based Access Control.

Keywords – Neutrosophic Similarity Measures, Cybersecurity Protocols, Accuracy, Data Security, Anomaly Detection.

I. INTRODUCTION

The prevalent digitization of learning environments, particularly within specific domains, such as Indoor Design (ID) courses of study, has made it more challenging to establish precise educational standards. When compared to standard linear methods used in traditional tests, novel applications require more complexity. Analysis designs are made more challenging by the fact that securing private data from being analyzed by attackers [1-6] is a significant problem.

To evaluate ID courses successfully, researchers must now attack a balance between demanding proficiency in technology from learners and providing them with sufficient room for Innovative Thinking Skills (ITS) [7–10]. A state of uncertainty, ITS, and emotion are just a few of the many factors that can make courses involving ID challenging and complex, which makes them problematic for standard evaluation methods to understand honestly. The collective number of online study materials used in ID education requires robust security measures to ensure their authenticity and privacy [11–14].

Neutrosophic Set Theory (NET) is an analytical model that describes a comprehensive method for addressing complex test concerns. By integrating the TMF (Truth-Membership Function), IMF (Indeterminacy-Membership Function), and

FMF (Falsity-Membership Function) from Fuzzy Set Theory (FST), it presents a higher method for analyzing ID courses with variable probability levels and different measurements.

The digitization of learning materials has presented cybersecurity challenges at the cutting edge as higher education institutions deal with a massive volume of sensitive data. Unauthorized access, data hacking, and test use can all be addressed with proper security measures.

The research results of the present investigation validate that a hybrid model, incorporating cybersecurity protocols and Neutrosophic Similarity Measures (NSM), should be implemented to enhance the accuracy and reliability of quality analysis within the context of higher education authenticity. By providing Confidentiality, Integrity, and Availability (CIA), the Cyber-Neutrosophic Model (CNM) enhances the review process, making it more robust and secure.

This Study Enhances the Assessment of Learning, As Well As Privacy and Security, In Multiple Directions.

- A more advanced method for addressing problems with innovative analysis has been implemented by integrating NST into ID education tests.
- This model proposes a comprehensive cybersecurity solution featuring Anomaly Detection (AD), access control, and encryption designed explicitly for learning environments.
- An integrated model has been effectively used and proved to be effective at a top ID institution in the case study.
- The remaining portions of the article have been organized as follows: Section 2 lays out the literature review that supports the proposed CNM. While Section 3 details the recommended approach, Section 4 provides the field experiment setup. The investigations' results and analyses are presented in Section 5, and the conclusions, along with the resulting implications for practice and future research directions, are drawn in Section 6.

II. THEORY

NST and Measures

An advanced version of conventional and fuzzy sets, NSTs are developed to address real-world problems that involve uncertainty, imprecision, and inconsistency. Applications such as quality in education rating and Decision-Making Systems (DMS) help from their application of the following factors: truth, indeterminacy, and falsity.

An NST as set $'A'$ in a universal set $'S'$ is formally defined by a truth-membership function $'TMF_A'$, an indeterminacy-membership function $'IMF_A'$, and a falsity-membership function $'FMF_A'$. For any element $'x \in S$', these functions provide values within the real interval [0,1]. Specifically, an NST as set $'A'$ can be expressed as Eq. (1).

$$A = \{\langle x, TMF_A(x), IMF_A(x), FMF_A(x)\rangle \mid x \in S\}, \tag{1}$$

Where,

- $TMF_A(x)$→ The degree of truth of $'x'$ belonging to $'A'$,
- $IMF_A(x)$→ The degree of indeterminacy of $'x'$ belonging to $'A'$,
- $MFF_A(x)$→ The degree of falsity of $'x'$ belonging to $'A'$.

These three values are not unavoidably dependent on each other, and in a general NST, they satisfy Eq. (2).

$$0 \le T_A(x) + I_A(x) + F_A(x) \le 3. \tag{2}$$

The flexibility of NST results in suitable methodologies that utilize non-binary decisions, enabling it to evaluate multiple proofs and uncertainty. The data factors and indicators of resemblance presented by NSTs allow us to measure the volume of data in an NST or the degree to which two NSTs are similar, both of which are important when measuring the quality of networks that must deal with uncertainty and missing data.

To measure the similarity between two NSTs as sets $'A'$ and $'B'$, this study can define an NSM as $S(A,B)$.

Let $A = \{\langle x_i, T_A(x_i), I_A(x_i), F_A(x_i)\rangle\}$ and $B = \{\langle x_i, T_B(x_i), I_B(x_i), F_B(x_i)\rangle\}$ for $i = 1,2,\ldots,n$. The similarity between A, B can be computed using the Eq. (3):

$$S(A,B) = \frac{1}{n}\sum_{i=1}^{n}\left[\frac{T_A(x_i)\cdot T_B(x_i)+I_A(x_i)\cdot I_B(x_i)+F_A(x_i)\cdot F_B(x_i)}{\sqrt{(T_A(x_i)^2+I_A(x_i)^2+F_A(x_i)^2)(T_B(x_i)^2+I_B(x_i)^2+F_B(x_i)^2)}}\right]. \tag{3}$$

This measure incorporates TMF, IMF, and FMF into an accurate metric by evaluating the similarity between two sets synchronously. NST, as defined in Eq. (4), can quantify data within a set, specifically set 'A'.

$$I(A) = \sum_{i=1}^{n}\left[TMF_A(x_i)\mathrm{Log}\ TMF_A(x_i) + IMF_A(x_i)\log\ I_A(x_i) + FMF_A(x_i)\mathrm{Log}\ FMF_A(x_i)\right] \tag{4}$$

Where,

- Data accuracy, indeterminacy, and error are tested empirically using the logarithm of the data.
- Particularly helpful when measuring the quality of education, where uncertain data is common, this parameter helps assess the accuracy and educational value of the dataset.

III. PROPOSED METHODOLOGY

Data Collection

The data collection process to assess the quality of ID education over two academic years [June 2022 to April 2024] from higher education institutions, covering four semesters, from undergraduate courses focusing on Design Fundamentals, Interior Space Design, and Graduation Design Projects. The dataset includes 327 student project records and 82 Tutor evaluation reports, showcasing students' participation in targeted courses over a specified period, encompassing design performance and educational quality components.

These Components Include

- 2D Drawings: The project involves creating floor plans and elevations that detail spatial layouts using software such as AutoCAD and Revit.
- 3D Models and Renderings: The visualizations were generated using SketchUp, 3Ds Max, and Rhino to showcase spatial concepts, material selections, and lighting design.
- Design Documentation: Technical reports on design, materials, and functionality.
- Presentation Videos: Students explain their design process and respond to feedback in 10–15-minute recorded presentations.

Each student project received 965 peer reviews (about three per project). Peer reviews provide qualitative feedback on ID, technical execution, and conceptual clarity [16-20]. Standardized reports were used to evaluate tutors.

Each Evaluation Includes

- Scoring Criteria: Predefined introductions are evaluated based on theoretical clarity, innovation, technical implementation, and visual quality to assign statical scores.
- Written Feedback: Qualitative feedback on strengths, weaknesses, and improvement.
- Observation Notes: Detailed tutor notes from in-class reviews and project reviews.

Additional information, known as metadata, included features such as task schedules, curriculum data, and aggregated demographic data, including learners' registration numbers, enrollment levels, and the duration of the study, which helped contextualize the key datasets within their surrounding environment.

Data collection was performed privately with the use of AES-256 for inputs and TLS 1.3 for communication. Securing access to the data repository for only authorized users was the primary objective in setting up Role-Based Access Control (RBAC). Additionally, Multi-Factor Authentication (MFA) was mandated as a mandatory requirement for all authorized users. This method guaranteed that the data would be secure, unaltered, and freely available at all times.

The security and integrity of all data, including applications and evaluation results, will be maintained by encrypting it using SHA-256. Additionally, it aggregated all Personally Identifiable Information (PII) following privacy standards and replaced student identification numbers with anonymous identifiers.

The audit logs recorded all data access and update tasks, providing security and control over data. Regular data backups were performed in the event of an emergency, and multiple versions of all data were stored on secure, cloud-based servers. The dataset, comprising 327 student assignments, 82 tutor assessments, and 965 randomly selected review data points (**Table 1**), provides a framework for assessing the quality of ID education using NSM and data-driven parameters.

Table 1. Detailed Dataset Description

Data Element	Type	Format	Unit/Range	Size	Quantity	Description
Project CAD Drawings	Spatial Design	DWG, RVT	Vector	50-150 MB	327 Files	Architectural floor plans and elevations created in AutoCAD/Revit include layering information and spatial measurements
3D Model Files	3D Geometry	SKP, MAX, 3DM	Mesh/NURBS	200-500 MB	327 Files	Complete 3D spatial models with materials, lighting, and camera settings
Design Reports	Text Document	PDF, DOCX	2000-5000 Words	5-20 MB	327 Files	Technical specifications, material choices, and design rationale documentation
Presentation Recordings	Video	MP4	10-15 Minutes	100-300 MB	327 Files	HD (1920 × 1080) video presentations with audio at 30 *fps*
Instructor Scores	Numeric	SQL	0-100 Scale	1-2 MB	82 Records	Quantitative evaluations across 15 assessment criteria

Instructor Comments	Text	SQL	200-1000 Words	0.5-1 MB	82 records	Qualitative feedback on project strengths and areas for improvement
Observation Notes	Text	SQL	100-500 Words	0.5-1 MB	82 Records	In-class critique documentation and progress monitoring
Peer Review Scores	Numeric	SQL	1-5 Scale	0.2-0.5 MB	965 Entries	Structured peer assessments across 10 evaluation criteria
Peer Comments	Text	SQL	50-200 Words	0.1-0.3 MB	965 Entries	Unstructured peer feedback and suggestions
Project Timeline Data	Timestamp	SQL	ISO 8601	0.1 MB	327 Records	Submission dates, revision history, and milestone completion times
Course Metadata	Mixed	SQL	Varied	0.5 MB	12 Records	Course objectives, teaching methods, and enrolment statistics
Student Demographics	Categorical	SQL	Encoded	0.1 MB	327 Records	Anonymized

NSM and Information Measure Calculation

Data and similarity parameters generated using the CNM are key in determining the success rate of ID courses. The above methodology provides robust and thorough assessments by defining data connections and material while considering uncertainty, unpredictability, and variance in evaluation.

Step 1: Representation of Data in Neutrosophic Form

First, transform the 327 student projects and 82 tutor evaluations into an NST. Student projects and evaluation scores have three membership functions:

- $TMF(x)$: Degree of example measure compliance.
- $IMF(x)$: Lack of clarity in measuring the situation.
- $FMF(x)$: Degree of noncompliance.

A tutor may rate a student project based on inventiveness using Eq. (4).

$$x_i = \langle T(x_i), I(x_i), F(x_i) \rangle = \langle 0.8, 0.1, 0.1 \rangle \tag{4}$$

- Signifying a high degree of TMF, low IMF, and low FMF.

Step 2: Defining Similarity Measure Between Two NST Sets

To compute the comparison between two NST sets $\{A, B\}$, Eq. (5) and Eq. (6)

$$A = \{\langle x_i, T_A(x_i), I_A(x_i), F_A(x_i) \rangle\} \tag{5}$$

$$B = \{\langle x_i, T_B(x_i), I_B(x_i), F_B(x_i) \rangle\} \tag{6}$$

For each element $'x_i'$ in the sets, $'A'$ and $'B'$, the similarity measure $S(A, B)$. This alignment between the TMF, IMF, and FMF degrees of corresponding elements in the sets provides a comprehensive measure of similarity under uncertainty.

Step 3: Computing Neutrosophic Information Measure

The neutrosophic data measure quantifies the information or uncertainty contained in a neutrosophic set. For a neutrosophic set $'A'$ with elements $'x_i'$ as $\langle T_A(x_i), I_A(x_i), F_A(x_i) \rangle$, the data measure $'I(A)'$. This computes the entropy-like measure for each element, reflecting the degree of certainty and uncertainty encapsulated in the TMF, IMF, and FMF. The negative sign ensures the data measure is non-negative, consistent with the ideas of entropy in data theory.

Step 4: Aggregation of Similarity and Information Measures

The quality of ID education is evaluated by aggregated similarity and data measures across multiple projects and evaluations, providing insight into student performance and tutor evaluations and indicating overall certainty and uncertainty within the dataset.

- S_{total} → The aggregated similarity score
- I_{Total} → The aggregated data measure

$$S_{\text{total}} = \frac{1}{m}\sum_{j=1}^{m} S(A_j, B_j) \tag{7}$$

$$I_{\text{total}} = \frac{1}{m}\sum_{j=1}^{m} I(A_j) \tag{8}$$

Where,

- m→ The sum of student projects
- The quality and consistency of educational results can be measured using these aggregated scores.

Step 5: Interpretation and Analysis

The final step involves interpreting similarity and data measures to assess the quality of ID education. A higher Similarity Coefficient (SC) indicates better instruction and learning because student performance matches tutor intentions. Higher data measures (reflecting greater uncertainty) may indicate evaluation variability or inconsistent student performance, highlighting areas for improvement.

Cybersecurity Integration Process

The ID education quality assessment system is protected by a robust cybersecurity model, which includes encryption, secure access control, and AD, to ensure reliable system access and prevent unauthorized activities that could compromise the assessment process (**Fig 1**).

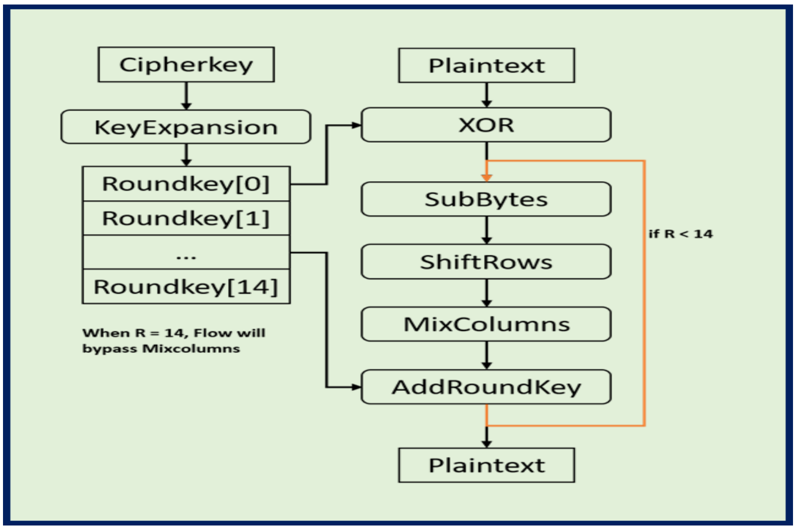

Fig 1. AES Encryption Standard.

Encryption

Encryption is crucial for data confidentiality and integrity throughout its lifecycle, including storage, transmission, and processing. In the proposed quality assessment system, the Advanced Encryption Standard (AES-256) is used to protect student projects, tutor evaluations, and peer review data. AES-256 operates on fixed-size blocks of 128 bits with a 256-bit encryption key, ensuring data remains unreadable even if unauthorized access occurs. The encryption method involves 14 rounds of transformations, including substitution, permutation, mixing, and key addition operations. The encoding, E(K, P), transforms PT into CT using the key 'K', while the encoding rebuilds the original text using the same key, ensuring only authorized entities can access the data.

A total of 14 evolution rounds, comprising key addition, mixing, substitution, and permutation, contribute to the data encoding. The encryption function denoted as $E(K, P)$, transforms the plaintext as PT into ciphertext as CT using the key $'K'$. Conversely, the decryption function $D(K, C)$ rebuilds the original PT from the CT using the same key. The data can only be accessed by authorized individuals who possess a suitable key, as outlined in these methods. Mathematically, the cryptographic method is Eq. (9).

$$C = E(K, P) \text{ and } P = D(K, C), \tag{9}$$

Where,

- CT→ Cipher Text
- PT→Plaintext
- K → 256-bit encryption key.

2D and 3D models, along with evaluation reports, are encrypted before being uploaded to a single repository within the CPM of the data storage process. The data encryption workflow begins with generating a random 256-bit key $'K'$ using a secure random number generator. The PT data $'P'$ is then encrypted with AES-256 to produce CT as $'C'$, which is subsequently stored in the repository. A Key Management System (KMS) is implemented to track the encryption key, ensuring that only authorized systems administrators are permitted to use it. The CPM generates, changes stores, and logs who has obtained the key.

Data transmitted between the test server and the Learning Management System (LMS) is encoded using a Transport Layer Security (TLS 1.3) secured channel. To prevent eavesdropping and Man-in-the-Middle (MiTM) attacks, TLS 1.3 establishes a secure connection through a handshaking protocol that includes authentication and key exchange. Until the message reaches the authorized sender, who can decode it with a valid key, the encrypted data is inaccessible. To maintain data security, Hash Functions (HFs) that use cryptography, such as SHA-256, generate unique hash values for each file. A distinct hash value has been generated by unauthorized data modification, enabling the detection of tampering. From data collection and encryption using AES-256 to secure storage or communication via TLS 1.3 with authorized users and, ultimately, decryption using a key managed by the KMS, the data lifecycle of data encryption is a dynamic process.

This workflow can be expressed as: Data Collection → AES-256 Encryption → Encrypted Storage/Transmission → Decryption upon Authorized Access.

Only authorized users will be able to access the encrypted data due to the stringent access control mechanisms employed in the method, such as Multi-Factor Authentication (MFA). For transparency and accountability, detailed audit logs track all cryptographic methods, providing a measurable record of when and by whom the data was obtained.

Secure Access Control

RBAC is applied by the testing platform to control user access to private data. RBAC assigns access privileges based on predefined roles, minimizing unauthorized access and ensuring users can only perform actions relevant to their system responsibilities.

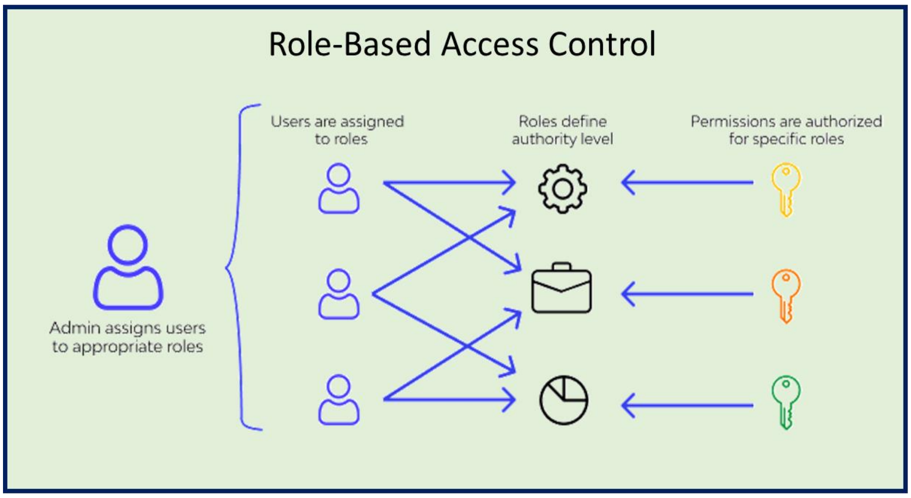
Role-Based Access Control
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

Fig 2. RBAC.

The proposed assessment system consists of four roles: students, tutors, administrators, and researchers. Each role has specific access rights and restrictions to maintain data confidentiality and integrity. Students have limited permissions to interact with their data, submit project files, view feedback, and access evaluation reports while being restricted from accessing or modifying data belonging to other students or administrative functions (**Fig 2**).

Mathematically, the access for a student S_i, Eq. (10).

$$\text{Access } (S_i) = \{\text{Submit\_Project } (S_i), \text{View\_Feedback } (S_i)\} \tag{10}$$

Instructors have access to evaluate student submissions, view class performance data, and provide feedback but are limited to modifying system configurations or accessing administrative data, excluding projects of students enrolled in their courses.

For a tutor $'I_j'$, access is defined as:

$$\text{Access } (I_j) = \{\text{Evaluate\_Project } (S_i), \text{View\_Class\_Performance } (I_j), \text{Provide\_Feedback } (S_i)\}. \tag{11}$$

Administrators hold the highest level of access control within the system. They manage system configurations, user accounts, and access permissions. Administrators can create, update, and delete user roles, ensuring system security by configuring encryption settings and reviewing audit logs.

The access rights of an administrator A_k are expressed as Eq. (12).

$$\text{Access } (A_k) = \{\text{Manage\_Users, Configure\_System, Access\_Audit\_Logs }\}. \tag{12}$$

Researchers have access to anonymized datasets for analytical purposes but are restricted from modifying the original records or accessing identifiable data about students or tutors.

For a researcher R_m, access rights can be defined as Eq. (13)

$$\text{Access } (R_m) = \{ \text{ Access\_Anonymized\_Data, Analyze\_Data } \}. \tag{13}$$

The model uses MFA to improve security beyond RBAC. It requires users to authenticate using two factors: a password and a one-time code sent to their registered device or email. This layered approach significantly reduces the risk of unauthorized access.

The authentication function for a user $'U'$, Eq. (14)

$$\text{Auth } (U) = \text{ Verify\_Password } (U) \wedge \text{ Verify\_OTP } (U). \tag{14}$$

Its access is granted only when the password verification (Verify_Password (U)) and one-time passcode verification (Verify_OTP (U)) are successful.

The system maintains detailed audit logs, tracking user access attempts and activities to ensure accountability and transparency by recording user ID, timestamp, accessed resource, and action performed. *e.g.,* An audit log entry for a student accessing their feedback might look like Eq. (15).

$$\begin{aligned}\text{Log } = \{ &\text{ User\_ID: "S12345", Timestamp: "2022-06-15 10:30:45",} \\ &\text{Resource: "Feedback\_Report", Action: "View" } \}\end{aligned} \tag{15}$$

Logs help administrators monitor user activity, detect suspicious behavior, and investigate potential security attacks. Reviewing these logs enables the detection of unauthorized access attempts and facilitates the implementation of corrective actions.

AD Using Isolation Forest Algorithm (IFA)

The AD detects potential security threats in data collected during the quality assessment method for ID education, ensuring the CIA of sensitive data, such as student projects, tutor evaluations, and peer review feedback, using the IFA.

The study utilized a dataset comprising 327 student project records, 82 tutor evaluation reports, and 965 peer review entries, which contained data on user activities, including submission times, file sizes, project revisions, and evaluation feedback, to identify probable AD. The data record is converted into a feature vector for the IFA, 'x_i', which contains key user interactions and data submissions.

The feature vector can be expressed as Eq. (16).

$$x_i = \langle f_1, f_2, f_3, f_4, f_5 \rangle, \tag{16}$$

Where,

- f_1 → Submission Timestamp-The time of project or evaluation submission.
- f_2→ File-The submitted project file or evaluation report (MB) size.
- f_3 → Number of Revisions-The number of times a project has been revised.
- f_4 → Evaluation Score-The score provided by the tutor.
- f_5 → Access Frequency-The total time of project or evaluation report has been accessed within a given period.

The IFA is trained on a dataset containing normal user behavior and data patterns observed during two academic years of study.

Let $X = \{x_1, x_2, \ldots, x_n\}$ as the dataset of feature vectors, where $n = 327 + 82 + 965 = 1{,}374$.

The IFA as $'F'$ is trained with $'T'$ isolation trees to establish a baseline of normal behavior, Eq. (17).

$$F = \text{ TrainIsolationForest } (X, T), \tag{17}$$

Where,

- T → The number of trees, typically set to 100 for optimal performance.
- During training, each isolation tree splits the data by randomly selecting a feature and a threshold value, isolating each data point.
- For each data point $'x_i'$ in the dataset
- IFA→ the path length $'h(x_i)'$, which is the number of splits required to isolate $'x_i'$.

The AD score $S(x_i)$ is computed as Eq. (18) to Eq. (20).

$$S(x_i) = 2^{-\frac{E(h(x_i))}{c(n)}}, \tag{18}$$

Where,

- $E(h(x_i))$→ The average path length across all isolation trees
- $c(n)$→ The normalization factor given by:

$$c(n) = 2H(n-1) - \frac{2(n-1)}{n} \tag{19}$$

with $H(i)$ representing the i-th harmonic number:

$$H(i) = \sum_{k=1}^{i} \frac{1}{k} \tag{20}$$

The AD score $S(x_i)$ lies between 0 and 1. If $S(x_i)$ is close to 1, the data point $'x_i'$ is likely to be an AD, indicating malicious activity. Conversely, lower scores suggest normal behavior.

Once the IFA is trained, it evaluates each new data record to AD. For an incoming feature vector $'x_i$', the AD score $S(x_i)$ is computed and compared against a predefined threshold $'\theta'$.

If the AD score exceeds $'\theta'$, the record is flagged as an AD by Eq. (21).

$$S(x_i) > \theta \Longrightarrow \text{ AD} \tag{21}$$

If a project submission is large or submitted outside of normal working hours, it may be considered an anomaly. Based on the severity of the attack, the network responds to ADs. System administrators may receive alerts, lock user accounts, or terminate suspicious sessions. Logging user ID, timestamp, and anomaly type for each AD.

For instance, an alert might be represented as Eq. (22)

Log Entry = ⟨User ID: "U123", Timestamp: "2023-09-15 14:32:10", Action: "Large File Submission", AD Score: 0.97⟩ (*22*)

Real-time AD derives from the IFA's low processing cost in AD. By using this approach, the system can quickly find and mitigate security attacks, ensuring the integrity and security of ID education reviews. Cybersecurity measures can be easily incorporated into the assessment system's workflow to ensure End-to-End security.

The Comprehensive Process Includes

- Data Submission: Students submit their projects via a secure, encrypted channel.
- Storage and Processing: Data is encrypted and secured; tutors use RBAC permissions.
- Evaluation: Instructors submit evaluations, which are encrypted and stored.
- Anomaly Monitoring: Activity is monitored and AD by the system.
- Access Logging: Every user action is logged for accountability and auditing.

By implementing encryption, secure access control, and AD, the cybersecurity integration method ensures the confidentiality, integrity, and availability of the ID education quality assessment system. This robust model secures sensitive data from unauthorized access and probable cyber-attacks, ensuring a secure and reliable assessment environment.

Algorithm: CNM Quality Assessment Model Inputs

- **Dataset D :** Consisting of $'n'$ student projects, tutor tests, and peer reviews.
- **Neutrosophic Parameters:** TMF, IMF, FMF.
- Encryption Key K (256-bit AES key).
- IFA as $'F'$ for AD.
- Threshold $'\theta'$ for AD.

Outputs:

- Aggregated SC as S_{total}
- Aggregated Data Measure I_{total}
- Anomaly Log L (AD)

1 **Data Collection and Preprocessing**
  - Collect the dataset $D = \{d_1, d_2, \dots, d_n\}$.
  - Perform data cleaning to handle missing values and outliers.
  - Standardize data to ensure consistency in formats, units, and scales.
  - Anonymize PII.

2 **Encrypt Data**

  For each data instance $d_i \in D$:
  - Encrypt d_i using AES-256: $C_i = E(K, d_i)$, where C_i is the CTof d_i.

3 Transform Data to NST

For each encrypted data instance $'C_i'$:

- FE to represent C_i as an NST as set A_i : $A_i = \langle T(C_i), I(C_i), F(C_i)\rangle$,

Where,

- $T(C_i), I(C_i), F(C_i) \rightarrow$ The TMF, IMF, FMF values.

4 Compute NSM

For each pair of NSTs, as $'A_i'$ and $'B_i'$ (student project and test):

- **Calculate the Similarity Measure $S(A_i, B_i)$:**

$$S(A_i,B_i) = \frac{1}{n}\sum_{j=1}^{n}\left[\frac{T_A(x_j)\cdot T_B(x_j)+I_A(x_j)\cdot I_B(x_j)+F_A(x_j)\cdot F_B(x_j)}{\sqrt{\left(T_A(x_j)^2+I_A(x_j)^2+F_A(x_j)^2\right)\left(T_B(x_j)^2+I_B(x_j)^2+F_B(x_j)^2\right)}}\right].$$

5 Compute Neutrosophic Data Measures

For each neutrosophic set $'A_i'$:

- Calculate the data measure $I(A_i)$:

$$I(A_i) = -\sum_{j=1}^{n}\left[TMF_A(x_j)\text{Log } TMF_A(x_j) + IMF_A(x_j)\text{Log } IMF_A(x_j) + FMF_A(x_j)\text{Log } FMF_A(x_j)\right]$$

6 Aggregate Results

- Compute the aggregated SC as S_{Total} :$S_{\text{Total}} = \frac{1}{m}\sum_{j=1}^{m} S(A_j, B_j)$

  where $'m'$ is the sum of project-evaluation pairs.
- Compute the aggregated data measure I_{Total} :$I_{\text{Total}} = \frac{1}{m}\sum_{j=1}^{m} I(A_j)$

7 AD Using IFA

- Train the IFA as $'F'$ on the dataset $'D'$ to compute a baseline for normal behavior:
  $F =$ TrainIsolationForest (D, T), where $'T'$ is the number of isolation trees.
- For each new data instance $'d_i'$, compute the AD score $S(d_i)$:$S(d_i) = 2^{-\frac{E(h(d_i))}{c(n)}}$

Where,

- $E(h(d_i)) \rightarrow$ The average path length for $'d_i'$
- $c(n)$ -> The normalization factor.

- If $S(d_i) > \theta$, flag $'d_i'$ as an AD and Log the AD: $L = L \cup \{d_i, S(d_i)\}$

8 Secure Access Control

- Implement RBAC to ensure only authorized users can access encrypted data and computed results.
- Apply Multi-Factor Authentication (MFA) for user authentication:
  Auth $(U) =$ Verify_Password $(U) \wedge$ Verify_OTP (U).

9 Generate Quality Assessment Report

- Compile the aggregated SC as S_{total} and data measure I_{total} into a comprehensive report.
- Include AD as L and corresponding security alerts.

IV. EXPERIMENTAL SETUP

The experimental setup for the proposed CNM quality assessment model integrates numerous tools, platforms, and software to help data processing, neutrosophic computation, and cybersecurity measures. The system's operation ensures accurate NSM and data measures while also securing the CIA through effective cybersecurity.

Implementation Details

The test used Python 3.9 for data analysis, Machine Learning (ML), and security protocols. NumPy and Pandas were used for statistical measures and data manipulation, while SciPy provided scientific analysis tools. For the IFA for AD, the Sci-Kit-LEARN library was used. To illustrate the results of the AD, data measures and resemblance tests, as well as charts and graphs, have been generated using Matplotlib and Seaborn. To enhance Python's features, R 4.2 was implemented for statistical analysis and validation of neutrosophic computations. While the ggplot2 technique is used to exhibit statistical patterns, the DPLYR package provides data manipulation functions. NSM and data measures have been proven to be reliable and accurate using R's statistical libraries. Amazon Web Services (AWS) provided the cloud architecture on which the network was founded, enabling scalable computing resources and secure storage solutions. With the help of Amazon Web Services' Elastic Compute Cloud instances, 327 student project files, 82 tutor tests, and 965 peer review entries were processed efficiently. With AWS S3, encrypted data was permanently stored, guaranteeing durability, availability, and secure access controls.

For data security, the OpenSSL library was implemented to establish the AES-256 encryption standard during the encoding process. Before being saved in the public cloud, data was encrypted to ensure privacy and prevent unauthorized access. TLS 1.3 secured information being transmitted between clients and servers from eavesdropping and Man-in-the-Middle attacks, and AWS-Key Management Service (KMS) securely protected encryption keys. Using Django's integrated authentication for user roles and access permissions, RBAC and MFA were integrated into a user interface and server system. To further enhance login privacy, MFA integrated password authentication with One-Time Passcodes (OTP). For ease and modularity, the AD component was deployed as a microservice on Docker containers. Kubernetes orchestrated these containers to ensure efficient load balancing and fault tolerance. IFA was used for this deployment. Network module design became simple with the help of the GitHub platform, which maintained the codebase's version control and collaboration. Continuous Testing and Deployment pipelines are enabled through GitHub Actions, providing accuracy and consistency. To ensure efficient data processing, neutrosophic computations, encryption, and AD task execution, the test setup was run on a Windows 10 operating system with an Intel Core i7 processor, 16 GB of RAM, and 512 GB of SSD storage.

V. RESULTS AND ANALYSIS

Analyzing the CIA of integrated cybersecurity systems, the recommended CNM quality review model for ID education will be evaluated using comprehensive parameters. This evaluation provides an accurate assessment of the method's features by evaluating its NSM and security measures' achievement.

Neutrosophic Evaluation Metrics

NSM Scores Across Models

The study reveals that different models, including the proposed CNM, Fuzzy Logic Model (FLM), Statistical Model (SM), and Support Vector Machine (SVM), have different capabilities in handling uncertainty and providing consistent evaluations for ID education quality assessment.

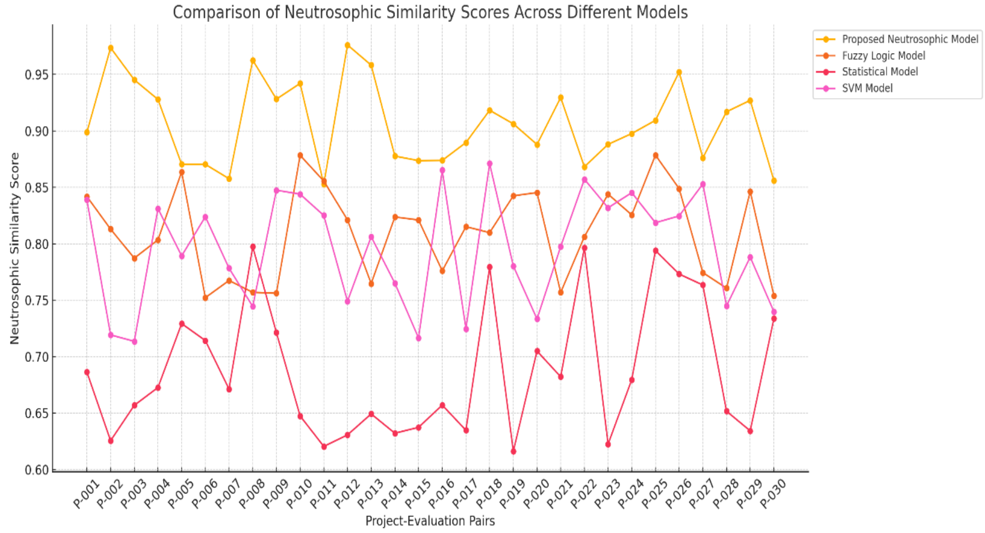

Fig 3. NSS Analysis.

There is a significant relationship between student work and tutor tests, which is demonstrated by the high SC (0.85-0.98) typically generated by the recommended CNM. **Fig 3** validates how this model improves upon others in terms of consistency and reliability and demonstrates its integration of TMF, IMF, and FMF to provide a comprehensive evaluation that more effectively addresses uncertainty and conflicting data.

The FLM, while capturing some uncertainty through TMF values, challenges the handling of IMF and FMF, thereby limiting its ability to represent the complexities of assessment data fully. However, that's not the case properly, despite not performing the CNM's comprehensive review.

Traditional methods of statistical analysis, such as variance and correlation, presume accurate data and disregard uncertainty as a factor; in contrast, the SM has lower similarity scores. This results in lower alignment between student projects and evaluations, highlighting the inadequacy of purely statistical approaches in uncertain environments.

The SVM classifies projects based on extracted features but lacks explicit management of uncertainty. Despite identifying data patterns, its deterministic nature limits its ability to handle ambiguous evaluations, making it a better alternative to the statistical model but still falling short of the proposed CNM.

Analysis of CNM Scores Across Models

The comparison of NSM scores across the Proposed CNM, FLM, SM, and SVM Models (**Fig 4**) reveals significant differences in how these models handle uncertainty, variability, and inconsistency in the assessment data for ID education. The Proposed CNM consistently generates the lowest data scores, typically ranging from 0.02 to 0.15. These low scores indicate that the model captures evaluations with minimal uncertainty, reflecting higher confidence and consistency in the data. The ability to explicitly manage TMF, IMF, and FMF allows the proposed CNM to reduce ambiguity and provide more reliable assessments.

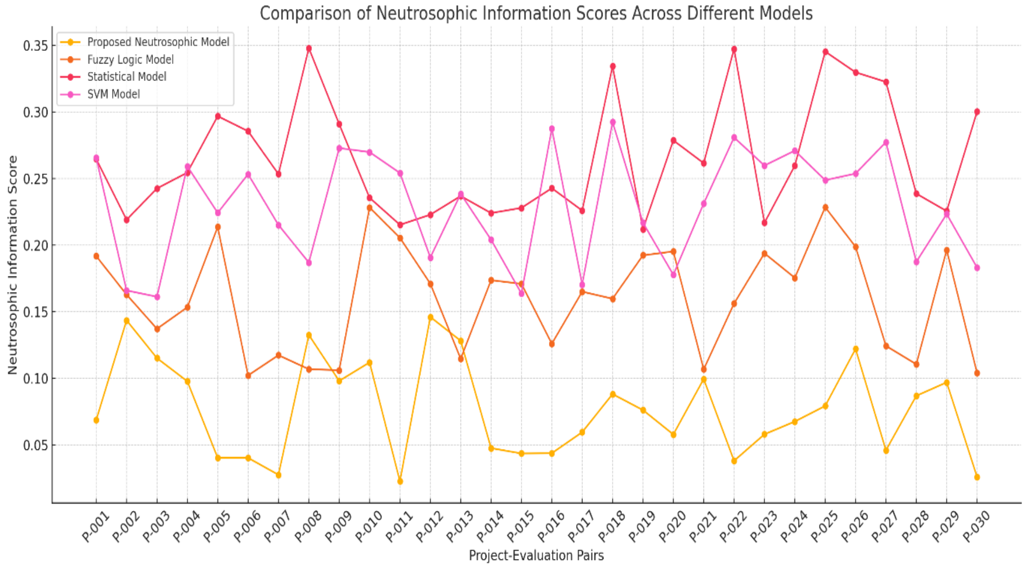

Fig 4. CNM Analysis.

The FLM generates higher data scores, ranging from 0.10 to 0.25. While fuzzy logic handles some uncertainty by TMF values, it does not explicitly incorporate IMF and FMF. Consequently, the model is challenged by more complex uncertainties, resulting in higher data scores and reflecting greater variability in evaluations.

The SM exhibits the highest data scores, 0.20 and 0.35. This result highlights the model's limited capacity to manage uncertainty, as traditional statistical methods assume precise data and do not accommodate conflicting data. The high data scores propose significant variability and inconsistency in the assessments when evaluated using purely statistical methods.

The SVM displays data scores between 0.15 and 0.30, indicating moderate uncertainty. The SVM classifies projects based on FE without explicitly addressing uncertainty. This leads to variability in the results, mainly when the data contains inconsistent tets. Although the SVM performs better than the statistical model, it still falls short of the proposed CNM's ability to minimize uncertainty.

Analysis of Consistency Ratios (CR) Across Models

The comparison of CR (**Fig 5**) against varying Similarity Thresholds provides insights into how well each model maintains alignment between student projects and tutor tests as the threshold for SC increases.

The Proposed CNM consistently achieves the highest CR across all SC, ranging from approximately 0.85 to 0.95. The model effectively handles uncertainty and produces consistent evaluations, even with severe SC, by incorporating TMF, IMF, and FMF into the CNM, thereby capturing nuanced data relationships for more reliable assessments.

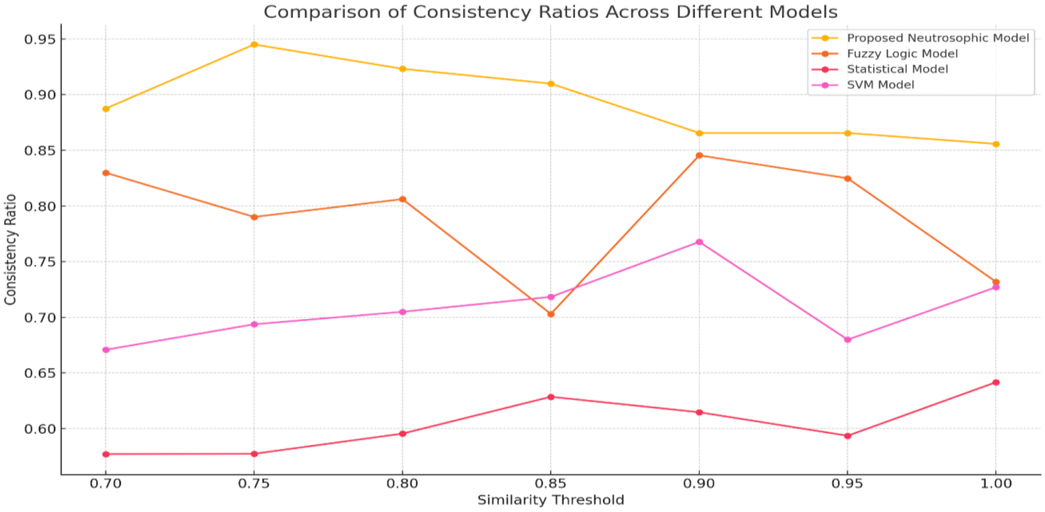

Fig 5. CR Analysis.

The FLM can measure a particular level of uncertainty by using TMF values; however, it cannot account for IMF and FMF, which restricts its accuracy under higher SC. Its performance drops off as the level of risk goes up, which means it can't handle significant uncertainties very well.

Due to its reliance on standard statistical measures that imply accurate data and are unable to account for conflicting tests, the SM has the lowest trust ratios, ranging from 0.55 to 0.70. This validates its failure to sustain coherence under uncertainty.

The classification of data using FE is where the SVM is obvious, displaying consistency ratios that are in the high SC range, from 0.65 to 0.80. Problems arise with uncertain ratings due to its predictive nature, which causes accuracy to decrease as the SC is decreased.

Cybersecurity Evaluation Metrics

Analysis of Security Mechanism Effectiveness Rates (SMER)

As the dataset size increases, SMER's ability to maintain data CIA distinct across the Recommended CNM, Basic Cybersecurity Model (BCM), RBAC-Only Model (RBAC-OM), and Anomaly Detection-Only Model (AD-OM) (**Fig 6**). The integration of AES-256 encryption for privacy of data, RBAC for secure access control, and IFA for AD provides that data is secured during storage, transmission, and access, and results in systematically high effectiveness SC ranging from 99.5% to 100% in the CNM.

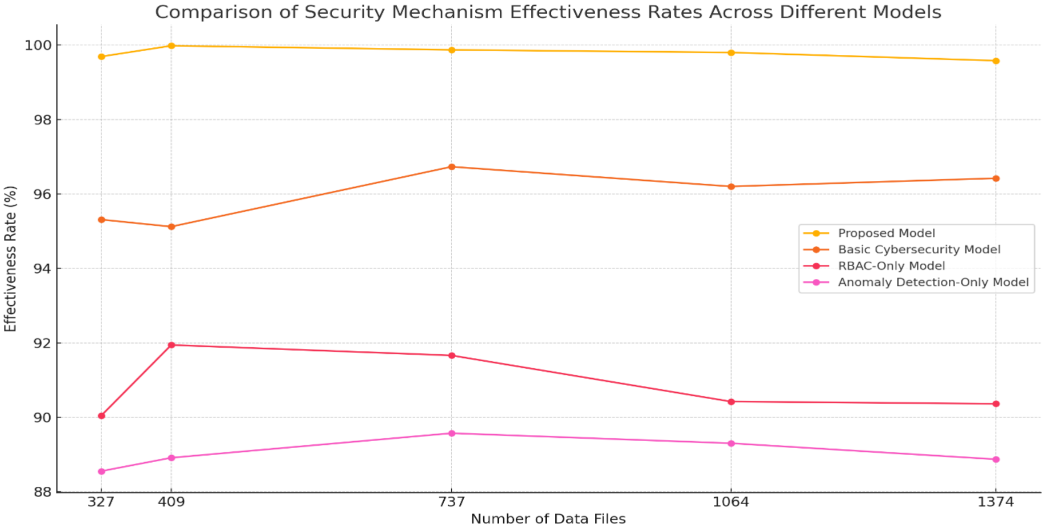

Fig 6. Security Mechanism Effectiveness.

By applying AES-128 encryption and primitive RBAC, the BCM is a CNM with Success Rates (SR) of 95% to 97%; however, it does not have improved AD. Although it isn't effective at detecting and responding to hacking attacks, it does a good task of controlling access to data and maintaining its secrecy. **Fig 6** illustrates that the RBAC-Only Model, which has an SR of 90% to 92%, is vulnerable to data breaches and unauthorized access because it emphasizes access control only, without encryption or AD.

While the AD-OM employs IFA for AD, it fails to include encryption for access control, but it does achieve SR ranging from 88% to 91%. The data becomes more vulnerable to attacks, and the probability of unauthorized access increases as a result. The SR of the BCM, RBAC-OM, and AD-OM decrease with increasing dataset size, demonstrating that they are not capable of processing larger datasets and ensuring total security. The recommended CNM remains highly successful.

Analysis of False Positive Rates (FPR) Across Models

The FPR of different methods, when compared to the Number of Normal Activities, is illustrated in **Fig 7**. The highly secure recommended CNM utilizes AES-256 encryption, RBAC, and IFA for AD to achieve an FPR of 0.5% to 1.5%. This helps minimize the number of FPRs by maintaining distinct lines between normal and abnormal behaviors. Since the BCM does not have advanced AD and uses less effective security features, it is more likely to flag common behaviors as abnormal, resulting in an FPR of 3.0% to 5.0%.

Because it focuses on access control without encryption or AD, RBAC-Only can incorrectly label legitimate use as malicious, resulting in a higher FPR. In contrast, the AD-OM's high FPR ranges from 2.5% to 4.5% because it can't use contextual access control mechanisms, lacks encryption for data, and thus enhances the risk of FMF labeling legitimate behavior as malicious. As the number of true activities increases, the BCM, RBAC-OM, and AD-OM models have challenges scaling up without compromising their accuracy. The Recommended CNM, on the other hand, maintains a low and stable false positive rate (FPR), implying that it is capable of handling larger datasets with a minimal number of false alarms.

Analysis of Response Times (RT) Across Models

The comparison of RT (**Fig 8**) across the Proposed CNM, BCM, RBAC-OM, and AD-OM highlights significant differences in AD speed and RT as the number of anomalies increases.

Using AES-256 encryption, RBAC, and IFA for Active Directory, the recommendation for CNM provides a response time of between 1.0 and 2.5 seconds. This succeeds by ensuring that Active Directory is secure and requests are processed, as well as optimizing the processes to minimize delays and enable real-time Active Directory and RT. RT with the BCM is lesser when compared with other models because it does not have robust AD and uses simpler security protocols.

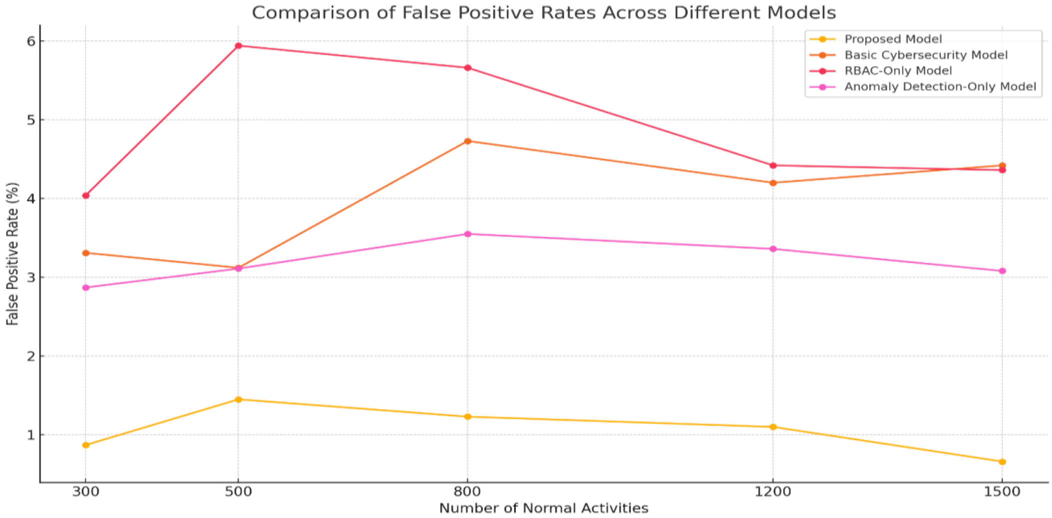

Fig 7. FPR Analysis.

The delay becomes clearer as the volume of AD increases, indicating that it is inadequate to handle higher security attacks effectively. On the other hand, the RBAC-Only has RT that ranges between 4.0 and 6.0 seconds, which leads to delayed identification and response times to anomalies. This is because there is no specific AD in the entire model. Although the AD-OM has RT that is not particularly fast, the fact that it lacks a cryptographic component makes it less secure. Although the BCM, RBAC-OM, and AD-OM as RT are showing an upward trend, they have encountered delays due to their limited capabilities and the lack of integration between encryption, access control, and advanced directory services. The recommended CNM can maintain low and stable RT robustness and capacity to scale in the context of an increasing number of anomalies.

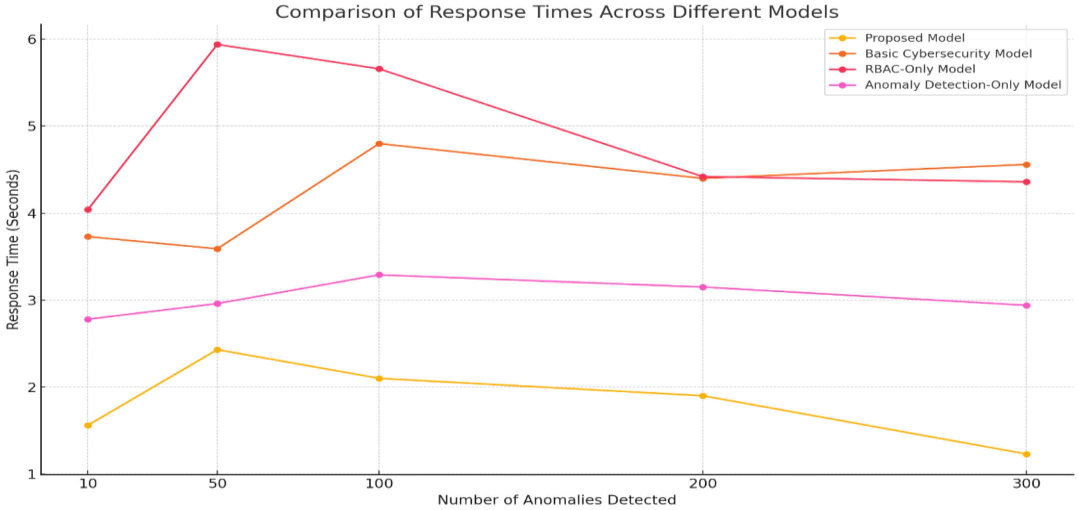

Fig 8. Analysis of AT.

VI. CONCLUSION AND FUTURE WORK

By demonstrating how neutrosophic mathematical concepts can be integrated into cybersecurity standards, this research highlights the potential for improving quality assessment in ID education. Using neutrosophic similarity scores that ranged from 0.85 to 0.98, the model achieved improved evaluation accuracy while ensuring robust data security through the use of AES-256 encryption and RBAC authorization. The model's practical applicability was validated with consistent performance across 327 student projects.

The current implementation of secure, mathematically robust educational assessment systems has proven successful in ID education. However, future research could explore its adaptation to other creative disciplines and institutional settings, serving as a model for modernizing evaluation processes while maintaining data integrity.

CRediT Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Manju A, Rukmani Devi S, Mohammed Alaa H Altemimi, Jwalant Baria, Arivazhagan D and Lakshmi Prasanna P; **Methodology:** Manju A, Rukmani Devi S and Mohammed Alaa H Altemimi; **Writing- Original Draft Preparation:** Manju A, Rukmani Devi S, Mohammed Alaa H Altemimi, Jwalant Baria, Arivazhagan D and Lakshmi Prasanna P; **Visualization:** Jwalant Baria, Arivazhagan D and Lakshmi Prasanna P; **Investigation:** Manju A, Rukmani Devi S and Mohammed Alaa H Altemimi; **Supervision:** Jwalant Baria, Arivazhagan D and Lakshmi Prasanna P; **Validation:** Manju A, Rukmani Devi S and Mohammed Alaa H Altemimi; **Writing- Reviewing and Editing:** Manju A, Rukmani Devi S, Mohammed Alaa H Altemimi, Jwalant Baria, Arivazhagan D and Lakshmi Prasanna P; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

[1]. A. Tleuken et al., "Which qualities should built environment possess to ensure satisfaction of higher-education students with remote education during pandemics?," Building and Environment, vol. 207, p. 108567, Jan. 2022, doi: 10.1016/j.buildenv.2021.108567.

[2]. P. Martins, S. I. Lopes, A. M. Rosado da Cruz, and A. Curado, "Towards a Smart &amp; Sustainable Campus: An Application-Oriented Architecture to Streamline Digitization and Strengthen Sustainability in Academia," Sustainability, vol. 13, no. 6, p. 3189, Mar. 2021, doi: 10.3390/su13063189.

[3]. M. Alenezi, S. Wardat, and M. Akour, "The Need of Integrating Digital Education in Higher Education: Challenges and Opportunities," Sustainability, vol. 15, no. 6, p. 4782, Mar. 2023, doi: 10.3390/su15064782.

[4]. S. Seoni, V. Jahmunah, M. Salvi, P. D. Barua, F. Molinari, and U. R. Acharya, "Application of uncertainty quantification to artificial intelligence in healthcare: A review of last decade (2013–2023)," Computers in Biology and Medicine, vol. 165, p. 107441, Oct. 2023, doi: 10.1016/j.compbiomed.2023.107441.

[5]. A. Akbar Firoozi and A. Asghar Firoozi, "Application of Machine Learning in Geotechnical Engineering for Risk Assessment," Machine Learning and Data Mining Annual Volume 2023, Dec. 2023, doi: 10.5772/intechopen.113218.

[6]. Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.

[7]. S. Sadrizadeh et al., "Indoor air quality and health in schools: A critical review for developing the roadmap for the future school environment," Journal of Building Engineering, vol. 57, p. 104908, Oct. 2022, doi: 10.1016/j.jobe.2022.104908.

[8]. A. Asadpour, "Student challenges in online architectural design courses in Iran during the COVID-19 pandemic," E-Learning and Digital Media, vol. 18, no. 6, pp. 511–529, Jun. 2021, doi: 10.1177/20427530211022923.

[9]. Bhutoria, A. (2022). Personalized education and artificial intelligence in the United States, China, and India: A systematic review using a human-in-the-loop model. Computers and Education: Artificial Intelligence, 3, 100068.

[10]. Al-Gerafi, M. A., Goswami, S. S., Khan, M. A., Naveed, Q. N., Lasisi, A., AlMohimeed, A., & Elaraby, A. (2024). Designing of an effective e-learning website using inter-valued fuzzy hybrid MCDM concept: A pedagogical approach. Alexandria Engineering Journal, 97, 61-87.

[11]. S. B. Veesam and A. R. Satish, "Design of an Iterative Method for CCTV Video Analysis Integrating Enhanced Person Detection and Dynamic Mask Graph Networks," IEEE Access, vol. 12, pp. 157630–157656, 2024, doi: 10.1109/access.2024.3485896.

[12]. Rawat, D. B., & Hagos, D. H. (2024). Metaverse Survey & Tutorial: Exploring Key Requirements, Technologies, Standards, Applications, Challenges, and Perspectives. arXiv preprint arXiv:2405.04718.

[13]. O. Aziz, M. S. Farooq, A. khelifi, and M. Shoaib, "Archaeometa: leveraging blockchain for secure and scalable virtual museums in the metaverse," Heritage Science, vol. 12, no. 1, Aug. 2024, doi: 10.1186/s40494-024-01416-w.

[14]. U. Mittal, S. Sai, V. Chamola, and D. Sangwan, "A Comprehensive Review on Generative AI for Education," IEEE Access, vol. 12, pp. 142733–142759, 2024, doi: 10.1109/access.2024.3468368.

[15]. D. Darío, P. H. Medina, and S. Yaman, "A Neutrosophic multi-criteria approach for implementing technology in education," International Journal of Neutrosophic Science, vol. 24, no. 4, pp. 245–256, 2024, doi: 10.54216/ijns.240418.

[16]. Shitaya, A. M., Wahed, M. E. S., Ismail, A., Shams, M. Y., & Salama, A. A. (2025). Predicting Student Behavior Using a Neutrosophic Deep Learning Model. Neutrosophic Sets and Systems, 76, 288-310.

[17]. S. Das, B. K. Roy, M. B. Kar, S. Kar, and D. Pamučar, "Neutrosophic fuzzy set and its application in decision making," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 11, pp. 5017–5029, Mar. 2020, doi: 10.1007/s12652-020-01808-3.

[18]. A. Abdelhafeez, A. E. Fakhry, and N. A. Khalil, "Neutrosophic Sets and Metaheuristic Optimization: A Survey," Neutrosophic and Information Fusion, vol. 1, no. 1, pp. 41–47, 2023, doi: 10.54216/nif.010105.

[19]. T. Fujita, "Advancing Uncertain Combinatorics through Graphization, Hyperization, and Uncertainization: Fuzzy, Neutrosophic, Soft, Rough, and Beyond," Dec. 2024, doi: 10.31224/4199.

[20]. О. Буров, О. Бутнік-Сіверський, О. Орлюк, and К. Горська, "Cybersecurity And Innovative Digital Educational Environment," Information Technologies and Learning Tools, vol. 80, no. 6, pp. 414–430, Dec. 2020, doi: 10.33407/itlt.v80i6.4159.