SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I1P118

Volume 13 Issue 1, 241-263, January 2026

Original Article

An Intelligent Blockchain Based Platform for Academic Fraud Prevention and Predictive Student Analytics Using CARTNet Model

Sangeetha A.S[1], Shunmugan S[2]

[1]*Department of Computer Applications, S.T. Hindu College, Nagercoil,*
Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India.
[2]*Department of Computer Science and Applications, S.T. Hindu College, Nagercoil,*
Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli, Tamilnadu, India.

[1]*Corresponding Author : asn.sangeetha84@gmail.com*

Received: 09 November 2025 Revised: 11 December 2025 Accepted: 10 January 2026 Published: 14 January 2026

Abstract *- The substantial dependence on an online method for maintaining academic records has raised concerns about data quality and the possibility of credential falsification due to flaws in centralized systems, such as brute-force attacks and cyber threats. Blockchain, configured with AES-256 encryption, provides a more effective and reliable approach for certifying academic records due to its ability to distribute data in a secure, decentralized manner and its resistance to hacking. Although combining blockchain technology with predictive modelling has remained extremely difficult, this proposal provides a unique approach to business models in education by merging the developing technologies associated with Deep Learning (DL) into a framework of academic management, along with a significant amount of blockchain-based secsurity and AES-256 encrypted protection of data. The proposed solution employs a new type of classifier, Chaotic-Attentive Recurrent Transformer-Net (CARTNet), which combines self-normalizing attention mechanisms with the dynamics of chaotic attractors for predicting student performance. Python software was implemented and evaluated for its performance using various metrics, including recall, accuracy, and precision. Also used a blockchain to protect the data sent between systems, and the validation of those records is conducted using the Java platform. Using these combined technologies to help create a reliable, expandable, and smart system. The system automates the confirmation of certificates and provides precise predictions of students' academic achievements. By providing companies and educational institutions with an accurate and validated set of data-based information for making decisions, this reduces the potential risk of fraud.*

Keywords *- Certificate Verification, Blockchain, AES-256 encryption, Chaotic-Attentive Recurrent Transformer Net.*

1. Introduction

With the advent of an internet-driven digital shift, a network-centric paradigm has occurred, resulting in the development of a new cybersecurity culture that has created significant levels of cybercrime and cybersafe activity to take place in the education systems of the world [1]. As such, Higher Education Institutions (HEIs) are a major source of demand for information technology products, provide education through faculty members, direct access to educational resources and facilities like the internet, all of which contribute to the HEIs supporting national development level objectives [2].

However, HEIs are also being targeted for academic fraud by those who seek to acquire credentials that exceed their own ability or level of education [3]. Academic Fraud is perpetrated by individuals who do not possess the required educational qualifications or training to support their aspirations for wealth, power, or recognition, or to gain employment [4].

Academic misconduct encompasses a variety of behaviours, including the unlawful modification of the original content of certificates of legitimate institutions to provide inaccurate claims [2]. Academic fraud is further defined as any activity where a person distorts or misrepresents his/her actual academic degree or credentials that ultimately harms other individuals, and includes any form of deceptive practice that involves people producing fake degrees from non-accredited or fraudulent academic institutions that present themselves as being legitimate, and therefore cannot award the degrees they claim to have issued [5]. As per [6], the sources of falsified degrees typically are not from officially recognised institutions but rather from

unrecognised institutions, so-called "credentialing companies" that produce fake diplomas and degrees, and people within the academic institutions who are fraudulent in their dealings. To manage these potential exposures, certificate verification is utilized to confirm the authenticity of the document and its owner. Verification verifies the issuer's credibility and ensures that the credentials are granted. These verification steps protect against fraudulent changes and ensure that the certificate is indeed associated with the correct person. Verification documents how the degree is awarded, and in doing so, authenticates the degree using accepted verification procedures. Degree certifications act as a means of confirming that an individual has successfully completed an established educational program [7]. Conventionally, universities have relied on manual processes for the issuance and verification of documents that are usually under the purview of examination offices or student affairs departments. Standard physical certificates (like paper-based records) mostly do not account for the full learner's profile, including the archival history and authentication. Open Badges and similar digital credentials have been created to overcome these shortcomings by offering a more adaptable and secure format. Nevertheless, the disadvantages of traditional methods have become increasingly visible because of the growth of education and the increasing demand for fast and reliable authentication. These disadvantages consist of inefficiencies in operations, processes that are prone to errors, and an increased risk of forgery of documents. In reaction to the frequent falsification of academic credentials, in which counterfeit diplomas and transcripts are included, educational institutions have turned more to online issuance of graduation certificates [8]. Though the digital method allows people to get documents from far away, it has also doubled the number of fake certificates that are being sent and used. The move to digital platforms has changed the way academic records are handled and has paved the way for automation and faster processes [9]. However, this change also brings the problems of data security, integrity, and very strict following of (Atomicity, Consistency, Isolation, and Durability) ACID. It is very important to make sure that these properties are followed to keep academic credentials authentic and trustworthy. Any breach may cause illegal access, data tampering, or the generation of forged certificates, which, in turn, result in the loss of trust and credibility of the institutions [10]. The previous discussion reveals that the existing academic record management systems and student performance prediction models are riddled with flaws. The problems stem from the security issues of a centralized system, lack of protection against fake certificates, and insufficient modelling of student behavior. A few publications have been developed to upgrade certificate verification or performance prediction. Nevertheless, very few have presented a complete, secure, and smart solution. These problems, which remain unsolved, pinpoint the research gap that this paper fills.

1.1. Related Works

This section explores modern studies concentrating on combining blockchain, powered verification systems with Machine Learning (ML) and DL, based automation models in the education sector.

Muhammad Nauman et al (2021) [11] have introduced a supervised ML method that used decision tree algorithms to obtain understandable decision rules from educational datasets, thereby allowing higher educational institutions to improve academic planning and student support with the help of data-driven predictions and pattern recognition. However, the findings yielded by the decision tree are affected by biases and errors in data labelling. Dhruvil Shah et al. (2021) [12] have implemented Extreme Gradient Boosting (XGBoost) and blockchain technologies in the education sector for the secure storage of student records and the reliable prediction of career trajectories after graduation, thereby seeking to eliminate the risks of counterfeiting and increase the trustworthiness of educational achievements. Nevertheless, the model is susceptible to overfitting, particularly if it is trained on noisy or imbalanced educational datasets. Mirna Nachouki et al (2023) [13] have presented the Random Forest (RF) algorithm to predict students' performance. The RF algorithm allocates the highest importance to the grades of the core subjects and builds several decision trees that vote together for the best predictions. The utilization of randomized data subsets at each node promotes diversity among the trees, thereby allowing the model to capture complex relationships in the data to predict academic success. However, RF suffers from decreased prediction accuracy due to the distribution of data being imbalanced across course categories; thus, it causes algorithmic bias to be introduced if feature groupings are disproportionate. Zaffar Ahmed Shaikh et al (2022) [14] have devised a system based on an Artificial Neural Network (ANN) driven DL technique combined with a decentralized blockchain framework for the security and storage of accreditation credentials. The system remarkably improves the resilience of credential classification and verification units. The method goes a long way in solving issues that have been haunting classification loopholes, detection inefficiencies, and instability in recognizing dynamic certificate evaluations across large candidate datasets for a long time.

Although the above-mentioned approaches have shown some ability, they are limited to traditional ML techniques that represent only a limited amount of complex behavior or simply collect and validate certificates without offering predictive intelligence support. Therefore, the proposed work overcomes the issues of the previously mentioned approaches and improves the model's effectiveness.

1.2. Research Gap

The previous research has made significant contributions to the areas of education through the development of data analysis techniques and tools to support certificate

authentication, receipt verification, and blockchain technology, but they still have limitations. Most approaches rely on traditional ML or shallow DL models, which have limited ability to capture complex behavioural dynamics. Blockchain-based systems primarily focus on storage and verification, with inadequate predictive intelligence. Furthermore, no existing framework offers an integrated solution that combines powerful DL-based student analytics and decentralized, cryptographically secure certificate administration. These restrictions motivated the creation of the suggested framework.

1.3. Motivation

The increased reliance on online systems for handling academic records has led to worries about data integrity, certificate forgery, and security lapses caused by centralized architectures. Current practices fail to offer strong security and intelligent prediction in one framework. This work is prepared as an approach to create a secure, decentralized, and intelligent academic management system that prevents data tampering and forged certificates using AES-256 encryption and Blockchain, and goes one step further to predict student performance using DL based CARTNet to help educational institutions make quality, data-based decisions. The contributions of the work are,

- AES 256 encryption is used to protect sensitive academic data and ensure no unauthorized access.
- Blockchain is used to support certificate validation, thereby limiting certificate tampering and reducing distrust in the integrity of academic records.
- The CARTNet model is used to predict student passing performance while providing institutions with support in data-based decision-making.

1.4. Overview of Paper Structure

Section II discusses relevant literature with a focus on the inadequacies of current academic record authentication mechanisms. Section III presents the system architecture proposed, where emphasis is laid on integrating blockchain technology with DL algorithms to provide better security and automatic verification. Section IV presents the experimental outcomes and measurement criteria, emphasizing performance, scalability, and the impact of DL models on data integrity and threat identification. Section V concludes the paper by reflecting on the findings and proposing areas for future research in secure and intelligent academic credentialing systems.

2. Proposed System Description

The proposed work involves the gathering of student data that involves academic, activity, and other types of information, as referenced in Figure 1. Also, the university has been generating students' certificate data. For privacy, confidentiality, and integrity, the certificate data are encrypted using the AES-256 algorithm and verified using blockchain, which offers a tamper-proof, decentralized authentication integration. If the validation process is successful, the certificate is either accepted or rejected based on the verification process.

At the same time, students' academic and activity information is loaded into the CART-Net classifier, which uses chaotic attractor dynamics integrated with self-normalizing attention to predict student performance.

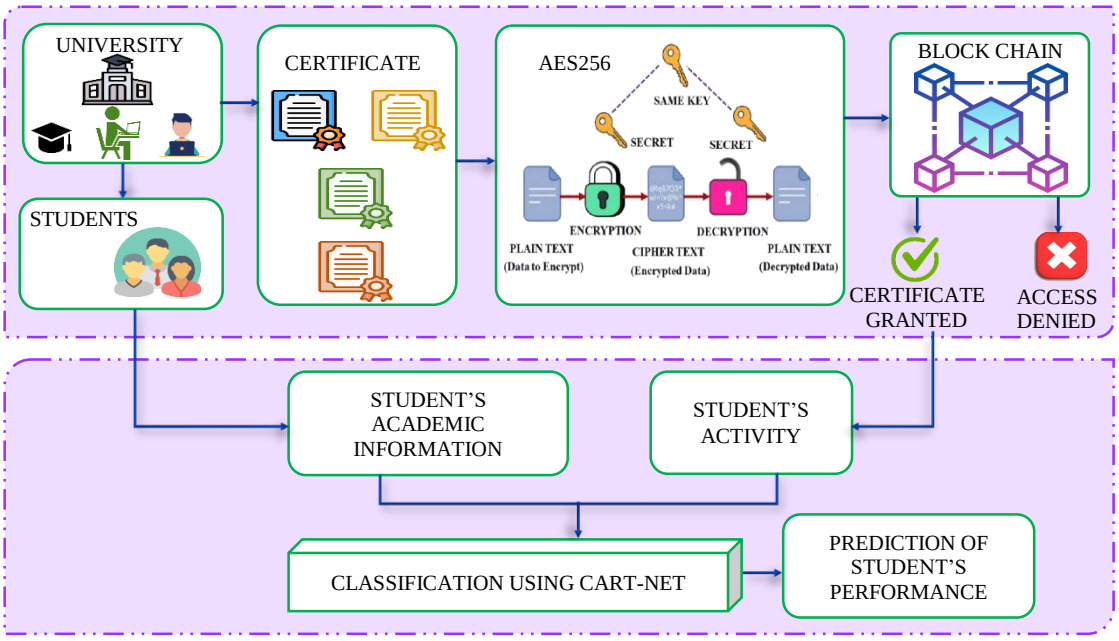

Fig. 1 Proposed block diagram

The performance measures are evaluated against typical measurements and are measured in terms of accuracy, precision, and recall. In conclusion, the duet process provides the university with secure certificate authentication, with blockchain and intelligent data predictive analytics using CART-Net to make credible, verifiable data choices by companies and institutions.

3. Proposed Methodological Framework

3.1. AES 256 Encryption Algorithm

The proposed academic fraud prevention framework utilizes AES 256-bit encryption to protect the academic records and prevent certificate forgery. AES encryption algorithm allows a Substitution-Permutation Network (SPN) structure and uses a key expansion process which applies an initial 256-bit key to generate round keys for 14 encryption rounds. AES-256 functions at fixed-size blocks of 128 bits (16 bytes), represented as a 4×4 byte matrix, making it a practical solution for securing structured academic data, including certificates, transcripts, and student records. The extended key length of AES-256 provides a key space, offering strong resistance against brute-force attacks. Figure 2 represents the structure of encryption. The AES-256 is realized with different encryption modes for protecting data in academic systems.

3.1.1. Electronic Code Book (ECB)

In ECB mode, as illustrated in Figure 3, each 128-bit data block is encrypted separately with the same AES-256 key. Therefore, every plaintext block is processed separately from the others and produces a corresponding ciphertext block.

3.1.2. Cipher Block Chaining (CBC)

Before being encrypted, every plaintext block is XORed with the previous ciphertext block. A randomized Initialization Vector (IV) is used in the initial block. This chaining ensures that the identical blocks of data produce different ciphertexts, making this mode ideal for protecting sequences of data. The Cipher Block Chaining mode process is shown in Figure 4.

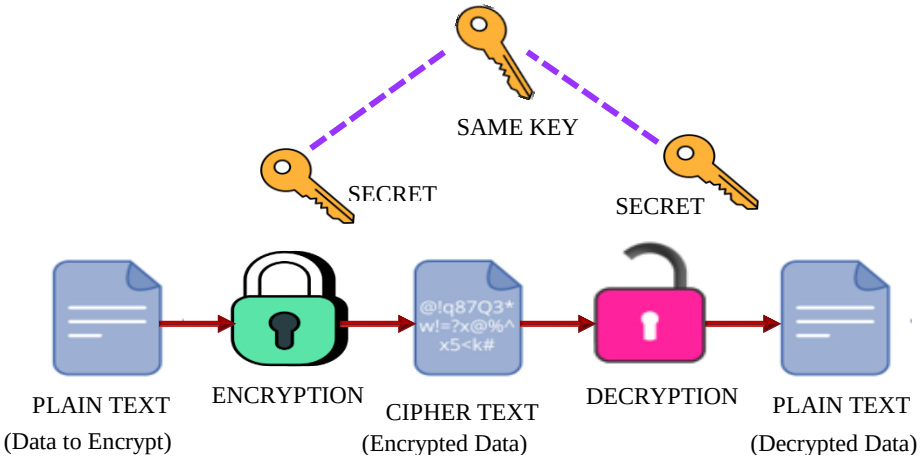

Fig. 2 Structure of encryption

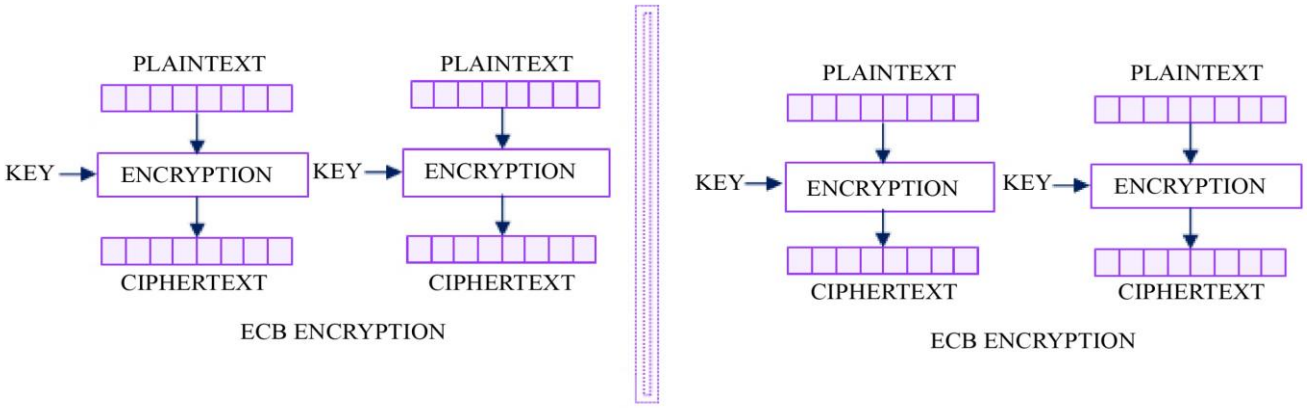

Fig. 3 Structure of ECB

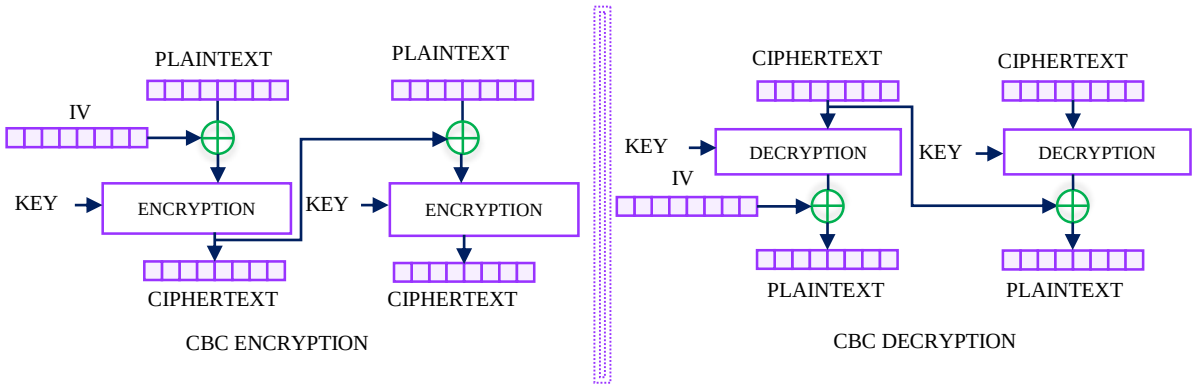

Fig. 4 Structure of CBC

3.1.3. Cipher Feedback (CFB)

CFB mode in Figure 5 allows encryption in smaller segments, effectively adapting the Block Cipher (BC) into a self-synchronizing stream cipher. Each plaintext segment is XORed with the keystream from the prior ciphertext block or IV. A ciphertext is generated for every piece of academic information that is stored or modified, making this system highly useful for meeting academic record-keeping requirements, including the ability to update continuously.

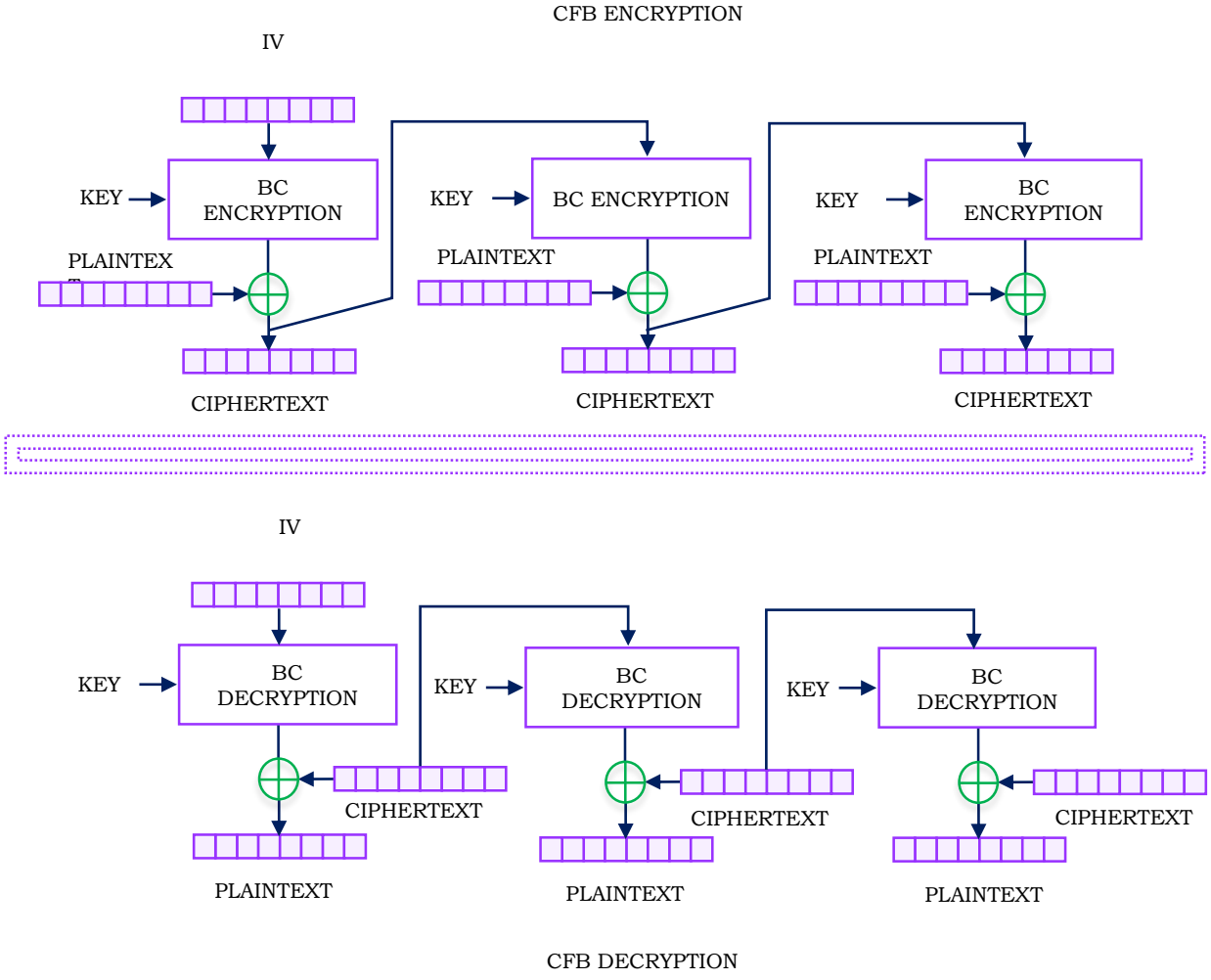

Fig. 5 Structure of Cipher feedback

3.1.4. Output Feedback (OFB)

The keystream produced by the BC in OFB mode, shown in Figure 6, is then XORed with the plaintext to create the ciphertext. The keystream is random and unrelated to both the plaintext and the ciphertext. This is one of the strengths of the encryption for streaming-type academic materials, and the fact that it can guarantee the security of any data transmitted in real-time.

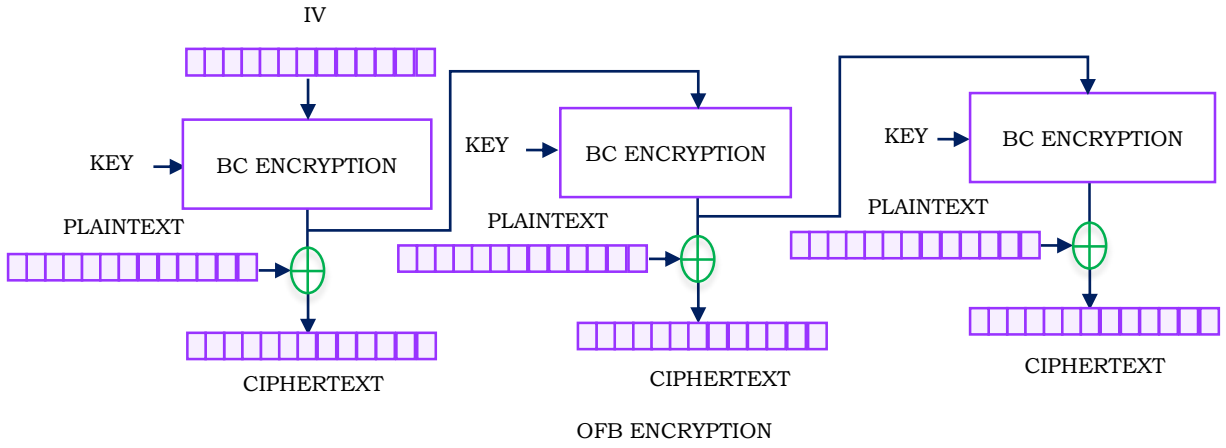

Fig. 6 Structure of output feedback

There are four main transformations in the encryption process that help secure the academic information.

3.1.5. Substitute Bytes Transformation

In this first transformation, an individual byte in the state is swapped with a different byte using a nonlinear S-box. This transformation uses Shannon's principles of diffusion and confusion to improve security through the avoidance of reused patterns.

3.1.6. Shift Rows Transformation

Each row of the state matrix's bytes is cyclically moved to the left in this second transformation. Without altering the state's overall size of 16 bytes, it rearranges the bytes within it. In addition to increasing the spread, the shift rows transformation makes defending against attacks more challenging.

3.1.7. Mix Columns Transformation

In Mix Columns, the scenario is repeated for each column in the state matrix, and an individual column of the state matrix is increased and combined using XORs. The effect is to diffuse each byte to the remaining states and strengthen the resultant cryptography against an attack on its structure.

3.1.8. Add Round Key Transformation

After Mix Columns, the round sub key (devised from the 256-bit key) is XORed into the state matrix, thereby binding the ciphertext to the key tightly. Thus, only a verified, authorized user with the correct encryption key can access, decrypt, and verify the object. The underlying structure of the state and the subkey is a 4×4 byte matrix, ensuring sufficient complexity to ensure integrity during encryption.

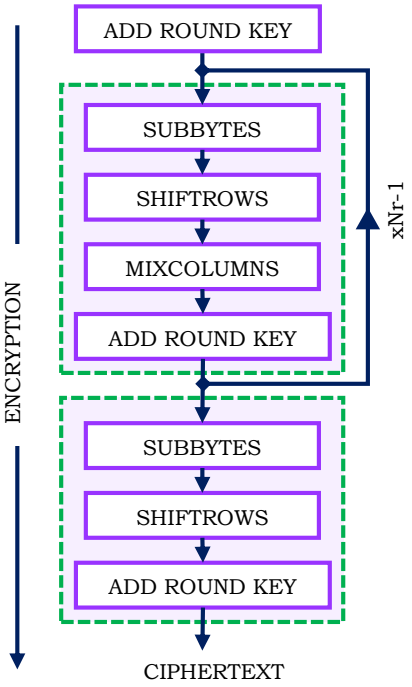

Fig. 7 Encryption process

By facilitating AES-256-based encryption as shown in Figure 7, it is deliberately ensured that academic credentials like certificates, transcripts, and other sensitive data are tamper-resistant, confidential, and verifiable, making it fundamentally obvious in enabling an important barrier for academic fraud and confirmed provenance of data. To enhance security, blockchain is used along with AES to store encrypted certificates in a tamper-proof and decentralized manner, certifying both privacy and integrity.

3.2. Blockchain

3.2.1. Functions Design in a Blockchain-Based Authentication System

An authentication system utilizing blockchain technology to prevent academic fraud is designed with the following functionalities.

3.2.2. Smart Contracts for Academic Data

Smart contracts are used to transfer academic information and confirm secure delivery. Smart contracts also confirm the user identity information, student or faculty, and also authenticate ownership of an academic resource, such as certificates and transcripts. The data storage in education for authentication is shown in Figure 8.

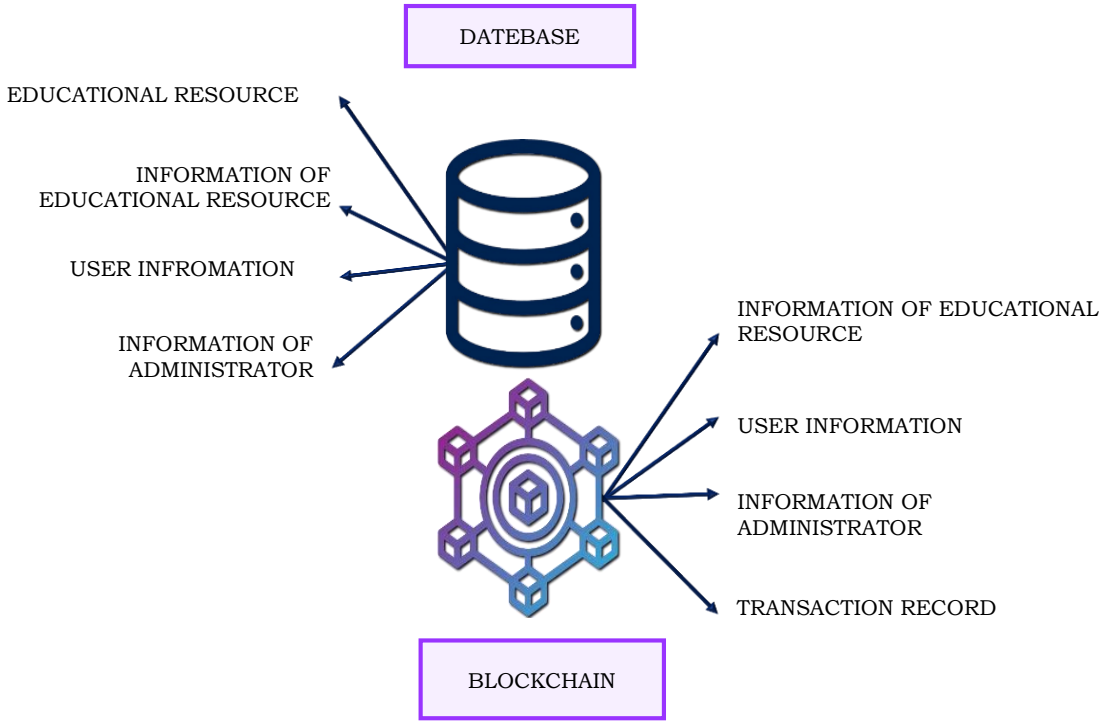

Fig. 8 Data storage for digital authentication in education

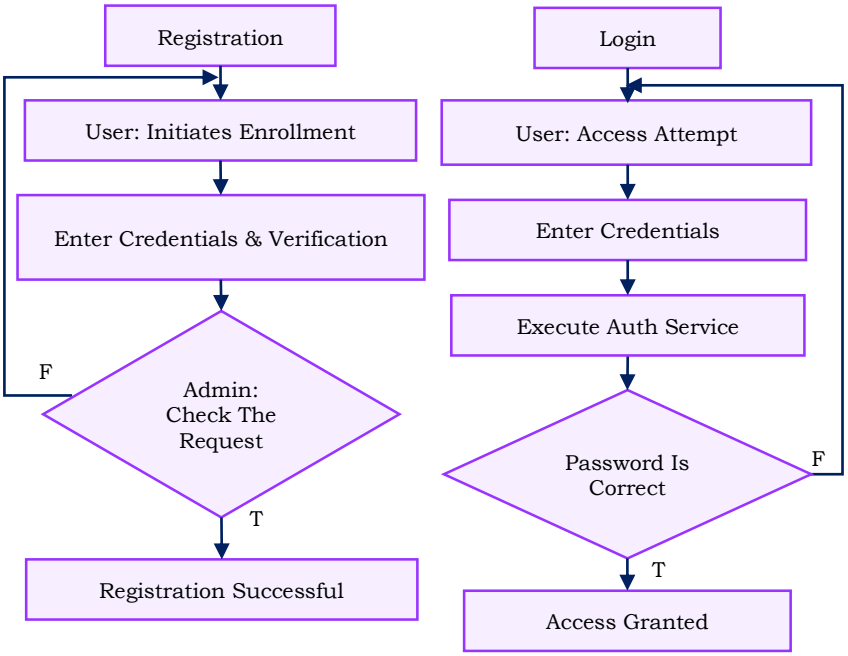

Fig. 9 Process of login and registration

3.2.3. Immutable Academic Records

When academic information is provided, it is recorded in both the blockchain system and a local database, ensuring accuracy and preventing tampering.

3.2.4. User Registration and Login

In the proposed system, user registration and login are leveraged with AES-256 encryption and blockchain-based smart contracts for security. Users are registered by providing their name, email, and password, as illustrated in Figure 9. The user's identity is encrypted using AES-256, and the encrypted user identity is sent over the network. If authentication fails, the user starts over again. Its Login is only successful when the encrypted identity matches the blockchain record.

3.2.5. Uploading Academic Resources

The platform permits the uploading of academic resources, whether it be certificates, assignments, or transcripts. Before placing resources into storage, they are encrypted using AES-256, and smart contracts are verified to ensure that the resource is appropriate. After approval, resources are permanently stored on the blockchain to protect against fraud, forgery, or unauthorized alteration. The file upload process is illustrated in Figure 10.

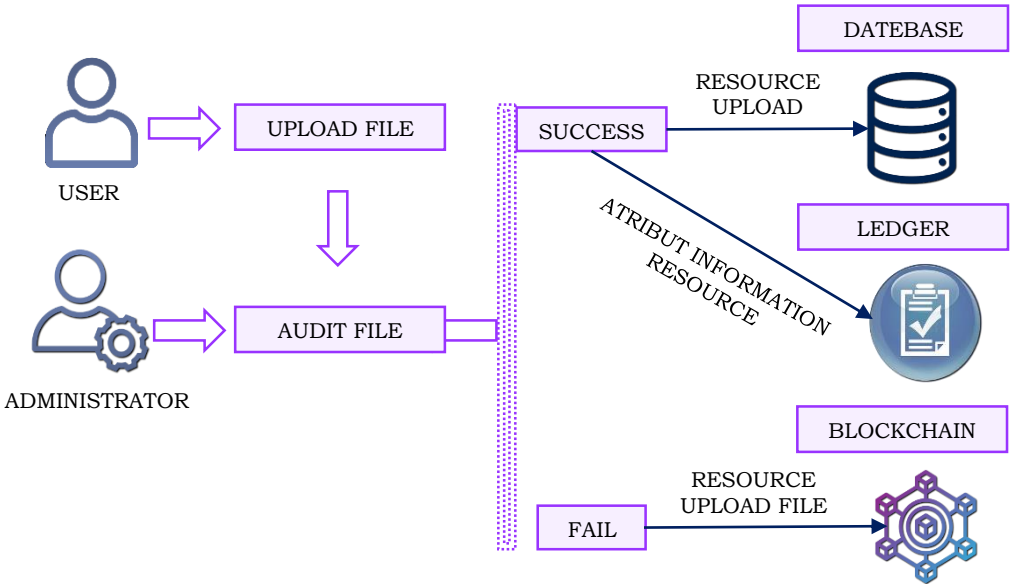

Fig. 10 Process of file upload

3.2.6. Downloading Academic Resource

When downloading resources, there are multiple verification safeguards. Based on blockchain records, identity verification is requested. User credential verification is completed through smart contracts, and AES-256 decryption ensures that the resource requested is legitimate. The academic resources can only be accessed by authorized users having valid blockchain permission, while unauthorized requests are denied. Process of data downloads as shown in Figure 11.

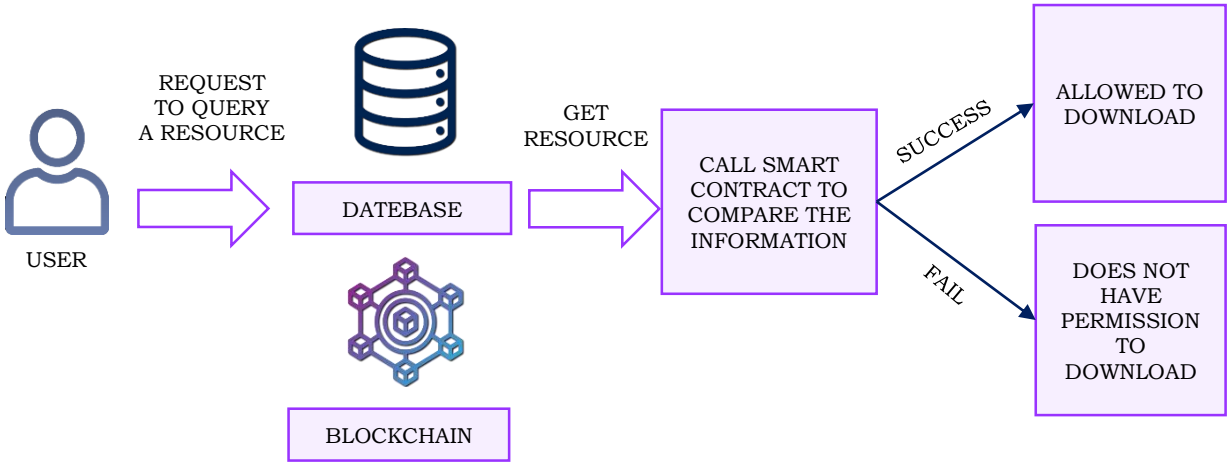

Fig. 11 Digital authentication data download

3.2.7. Administrator Role

Administrators are responsible for all user data, operations, and activities stored in the blockchain. They validate uploads of academic resources and verify ownership certification before data is permanently stored. If a document is falsified or does not pass AES-256 verification or is flagged by the blockchain, the academy rejects it, and it is removed from the academy's record.

Blockchain is a decentralized and distributed ledger that creates permanent or unchallengeable records of data in a transparent way. Each block of information contains academic content connected to the prior block using cryptographic hash functions. As records and data can no longer be falsified, trust, security, and transparency are enhanced in an academic management system that operates without relying on centralized authorities and a single point of failure. A blockchain-based platform designed for the security of certificates. Before the records are stored in the proposed solution, they are encrypted using AES-256 encryption for confidentiality. The records are then uploaded to the Interplanetary File System (IPFS), which produces a unique Content Identifier (CID). The CIDs are stored in the blockchain for immutability, preventing certificate forgery. In the verification of a certificate, the CID is matched with the entry in the blockchain, and the academic information associated with the CID is decrypted and validated. This process assures that academic certificates remain tamper-proof, transparent, and securely accessible.

The process for Admin/User enrolment and for block creation follows these steps:

1. Admin or User submits information, consisting of Name, Password, and Authority.
2. System verifies for completeness.
   - If complete → Unique ID is generated.
   - If incomplete, Invalid → Consumes request, request is denied.
3. Admin submits Academic information, data being AES-256 encrypted.
4. System is checking for blockchain balance:
   - If enough funds → A single block is created on the blockchain containing BCT_ID. The encrypted Academic data remains in IPFS.
   - If not enough funds → Consumes request and sends notification.

The enrolment process occurs when an admin or user submits their information, including name, password, and authority details. Verifying credentials is the first step; the system validates the provided user credentials. If the credentials are valid, a unique Identity (ID) is created for the user. If the credentials are invalid, the request is promptly rejected to prevent unauthorized access. Once authenticated, the admin uploads the academic records of a student, student details, or a certificate. Once academic documents are uploaded, the documents are encrypted using AES-256, which translates plaintext to ciphertext. This also keeps confidentiality, as even if the data is extracted, it remains interpreted without the proper decryption key. After encryption, the system proceeds to create a new blockchain block. This block contains the Blockchain Certificate ID (BCT_ID), which serves as a tamper-proof fingerprint of the record. While the block is permanently stored on the blockchain to ensure immutability, the encrypted academic data itself is uploaded to the IPFS for distributed and secure storage. This process has the added benefit of only permitting registered academic records to be associated with verified users. Furthermore, through the implementation of AES-256 encryption, Blockchain hashing, and IPFS storage, the records are kept confidential, authentic, and tamper-proof.

Algorithm for Certificate Issuance and Verification (Process Protocol)

1. Student submits details of certificate: Certificate Type, Issuer (University/College), Date, and Recipient Name.
2. Staff Authorized checks and verify details are then stored in the database.
3. The certificate is encrypted using AES-256, then moved to the blockchain, creating a Blockchain Certificate ID (BCT_ID).
4. Blockchain balance is verified through MetaMask.
   - If sufficient → then a new certificate block is created
   - If insufficient → then request denied
5. For verification, retrieve the certificate encrypted from IPFS using the BCT_ID.
6. The system decrypts the certificate and compares it to previous blockchain records.
   - If the match → certificate is verified
   - If no match → then permission denied.

The certificate issuance process begins the moment a user submits the certificate details, including the certificate type, the issuing institution (such as a university or college), the date, and the recipient's name. These details are verified by authorized academic staff to ensure authenticity. Once verified, the certificate data is encrypted using AES-256, ensuring confidentiality and tamper resistance for the certificate, just before being uploaded to the blockchain. Once the certificate has been encrypted, it is transferred to the blockchain by the system, which then creates a different and unique BCT_ID. The ID is permanent and unique; the BCT_ID acts as a digital fingerprint of the certificate. Again, the system checks the balance in the user's MetaMask wallet to authorize the transaction of transferring the encrypted certificate to the blockchain. If there are sufficient credits in the wallet, a new certificate block is created and added to the blockchain; if there are no credits available, the request is declined. At the verification step, the recipient or employer denies certification validation. The system retrieves the encrypted academic data from IPFS using the BCT_ID. The

data is decrypted using AES-256, and its integrity is validated against the hash stored on the blockchain. If the values match, the credential is authenticated and valid.

If there is a difference, it is a failure, and one will be denied. This guarantees that an academic certificate remains falsified, since each certificate issued is associated with the blockchain with AES-256 encryption.

3.3. Chaotic-Attentive Recurrent Transformer Net (CART-NET)

The CART-NET DL classifier is a hypothetical neural network architecture that uniquely combines chaotic attractor dynamics with self-normalizing attention methods, Recurrent Neural Networks (RNNs), and Transformer networks, as shown in Figure 12. In academic fraud prevention and predictive student analytics, chaotic attractors are used to represent the irregular, hidden, and non-linear behavioral patterns of learners.

Since chaos has fractal and sensitive characteristics, the system detects small changes in academic activity, robustly classifies between genuine and fraudulent activity, and predicts long-term academic activity trends in the lifetime of a student with more precision.

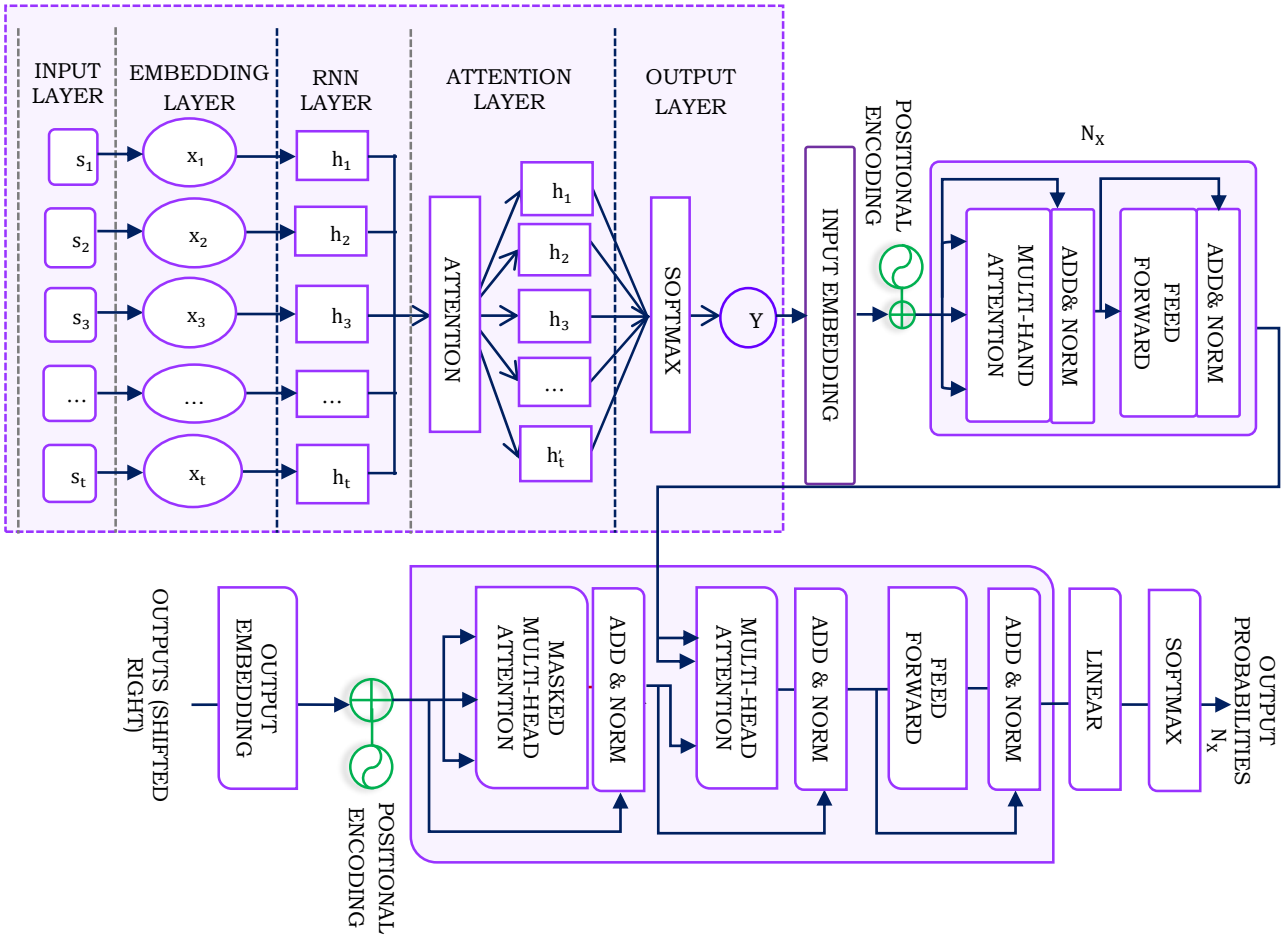

Fig. 12 Structure of the CART-NET DL classifier

The embedding of chaotic attractors into the analytic framework enables a deeper understanding of complex dependencies and temporal irregularities in student data, ultimately enhancing the reliability of fraud detection and predictive capabilities. Chaotic attractors, such as the Rössler and Rabinovich–Fabrikant systems, are used as nonlinear feature generators. The differential equations governing the Rössler attractor are:

$$\frac{dx}{dt} = -y - z \tag{1}$$

$$\frac{dy}{dt} = x + ay \tag{2}$$

$$\frac{dz}{dt} = b + z(x - c) \tag{3}$$

The system's behaviour is determined by three parameters (a, b, c), which control the amount of chaos

present. The states of the three variables (x, y, z) define how they evolve, reflecting a smooth motion with great sensitivity to small changes in terms of engagement with a student's academic activity, making it possible to detect hidden inconsistencies.

$$\frac{dx}{dt} = y(z - 1 + x^2) + x \quad (4)$$

$$\frac{dy}{dt} = x(3x + 1 - x^2) + y \quad (5)$$

$$\frac{dz}{dt} = -2z(\gamma + xy) \quad (6)$$

The parameter (γ) determines the rate at which the outputs of the system attractors exhibit sudden and chaotic behaviour. The system uses this characteristic to detect abrupt irregularities in student activity streams by detecting sudden changes in the number of failed login attempts. These outputs created from the system attractors are then combined with the original features to create enhanced input features.

$$Z_t = [x_t \oplus Rössler_t \oplus RF_t] \quad (7)$$

To address intricate dependencies hidden in disorderly input data, attention mechanisms are utilized. Chaotic attractors function to transform the raw academic data into discriminative features that highlight representational anomalies. Once the chaotic features are obtained, the attention mechanism is put into operation for analysis and detection. The attention mechanism is represented by query (Q), key (K), and value (V) as:

$$Q = XW_Q \quad (8)$$

$$K = XW_K \quad (9)$$

$$V = XW_V \quad (10)$$

Here, $W_Q, W_K, W_V \in \mathbb{R}^{d \times d_k}$ stands for trainable matrices. The attention mechanism determines the relationship between features by means of scaled dot, product attention:

$$Att(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (11)$$

Significant academic relationships are captured by normalizing and using similarity between queries and keys to obtain the corresponding values. This operation is further elevated by multi-head attention to identify various kinds of anomalies:

$$MHA(X) = Concat(Att_1, \ldots, Att_h)W_o \quad (12)$$

Here h stands for the number of attention heads, and W_o are the forecast output weight matrix. The model also includes normalization and residual connections to stabilize the training objective:

$$\tilde{X} = LN(X = MHA(X)) \quad (13)$$

The features are refined using a Feed-Forward Network (FFN):

$$X^+ = LN\left(\tilde{X} + FFN(\tilde{X})\right) \quad (14)$$

$$FFN(x) = max(0, xW_1 + b_1)W_2 + b_2 \quad (15)$$

Here W_1 *and* W_2 stands for weight matrices and b_1, b_2 are biases. An enhanced nonlinear representation of academic anomalies is achieved, where attention pooling is applied for sequence summarization using a learnable query vector q:

$$\alpha = softmax(q^\top X^+) \quad (16)$$

$$x^* = \sum_{t=1}^{T} \alpha_t X_t^+ \quad (17)$$

In this case, α_t are attention weights denoting the relevance of each student activity record, and x^* is a pooled feature vector that summarises the sequence.

Given that student performance indicators and fraud-related anomalies change over time, RNNs are ideal to represent these sequential patterns. At every time step t, the network receives an input vector x_t that represents chaotic-enhanced academic features, and updates its hidden state using:

$$h_t = \sigma_h(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (18)$$

Where. W_{xh} maps input features to a hidden representation, W_{hh} captures temporal recurrence, and b_h is the bias vector. The nonlinear activation function σ_h allows the model to capture complex, nonlinear dependencies in student performance and fraudulent behaviors. At each time step, the model computes the predictive or anomaly-related output given by:

$$y_t = \sigma_y(W_{hy}h_t + b_y) \quad (19)$$

Here W_{hy} maps the hidden state to the output space and b_y is the output bias, and σ_y stands for activation function. In this way, the RNN tracks students' performance trends while simultaneously signalling sudden disruptions that relate to potential academic fraud. In parallel, global dependencies are represented using a Transformer encoder. The input with positional encoding is represented as,

$$Z_n = Z + P \quad (20)$$

Here P is the positional embedding that preserves temporal order. The Transformer block uses Multi-Head Self-Attention (MSA) and Multi-Layer Perceptron (MLP) with residual pre-norm connections:

$$z_l' = MSA(LN(z_{l-1})) + z_{l-1} \quad (21)$$

$$z_l = MLP(LN(z_l')) + z_l' \quad (22)$$

MLP inside the Transformer applies the Gaussian Error Linear Unit (GeLU) activation:

$$MLP(x) = GeLU(xW_1 + b_1)W_2 + b_2 \quad (23)$$

$$GeLU(x) = x \cdot \Phi(x) = x \cdot \frac{1}{2}\left(1 + erf\left(\frac{x}{\sqrt{2}}\right)\right) \quad (24)$$

Here $\Phi(x)$ stands for a cumulative distribution function of a standard Gaussian distribution, and $erf(\cdot)$ is an error function. Final classification output is generated by mapping the pooled representation into label space:

$$\hat{y} = softmax(W_0 x^* + b_0) \quad (25)$$

Here W_0 and b_0 are the weights and bias for classification, and $\hat{y}$ is the probability distribution over classes. The objective function is cross-entropy loss:

$$L = \sum_{k=1}^{K} y_k \, log \, \hat{y}_k \quad (26)$$

Here y_k stands true label and $\hat{y}_k$ is the predicted probability for class k. CARTNet uses the architecture above to capture chaotic attractor dynamics, multi-head attention, recurrent modeling, and global encoding based on Transformers to produce high accuracy for academic fraud detection and predictive analytics.`

4. Results and Discussion

The proposed work is implemented using Python with the Students' Academic Performance Dataset for CARTNet to predict student performance, AES-256 encryption for student academic records, and blockchain together with the Java platform for certificate validation.

The experimental results show that the system provides secure and tamper-resistant record management while achieving appropriate accuracy, precision, and recall for predicting student performance.

Fig. 13 Home page of student analysis

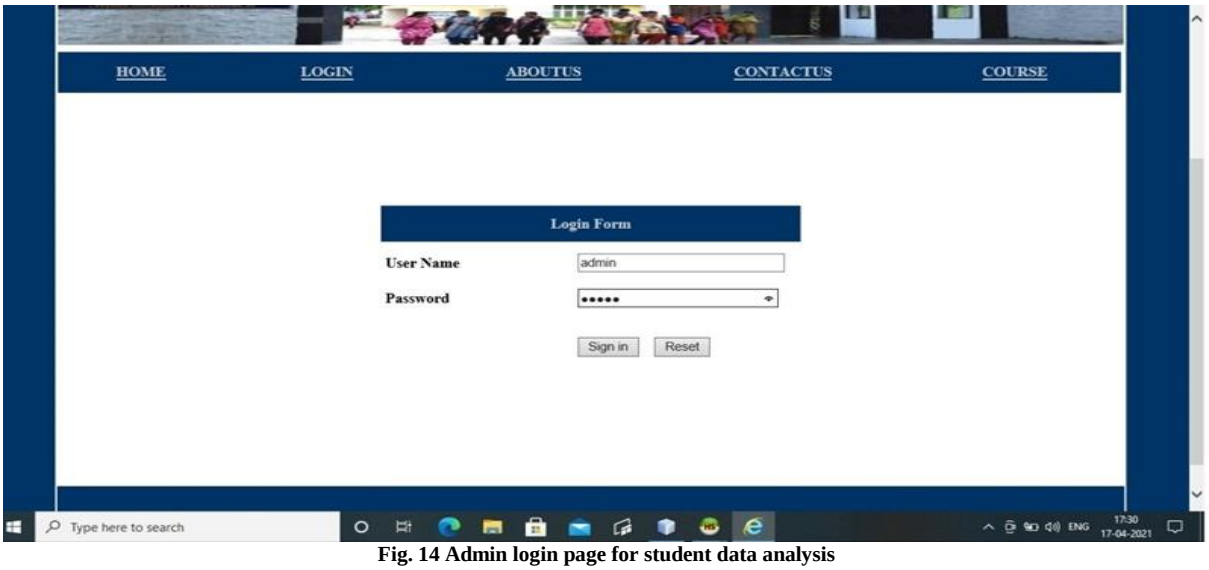

Fig. 14 Admin login page for student data analysis

Figure 13 represents the home page of the student result analysis and performance reporting system, showing navigation menus such as Home, Login, About Us, Contact Us, Course, and institutional information under the Faculty of Computer Science. It is the central entry point for student, staff, and administrators to access academic services, integrated with a secure system that uses AES-256 encryption and Blockchain-based authentication, ensuring the access and protection of academic data.

Figure 14 displays the admin login page for student result analysis and performance reporting system, on which a username and password are used to authenticate the user. This page offers the admin a secure access point into their administrative dashboard from which they manage staff, students, and all academic records. The credentials are encrypted using AES-256 before being submitted to the system, and verified through Blockchain authentication to establish data confidentiality and integrity.

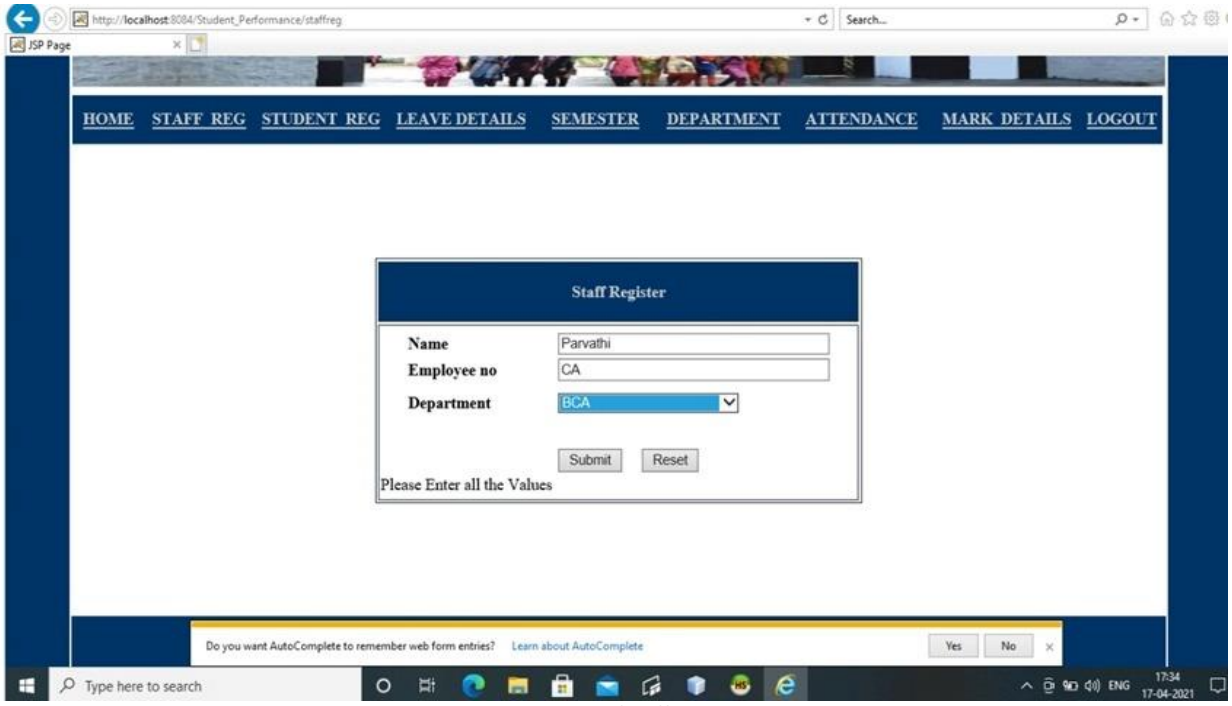

Fig. 15 Login page of staff registration

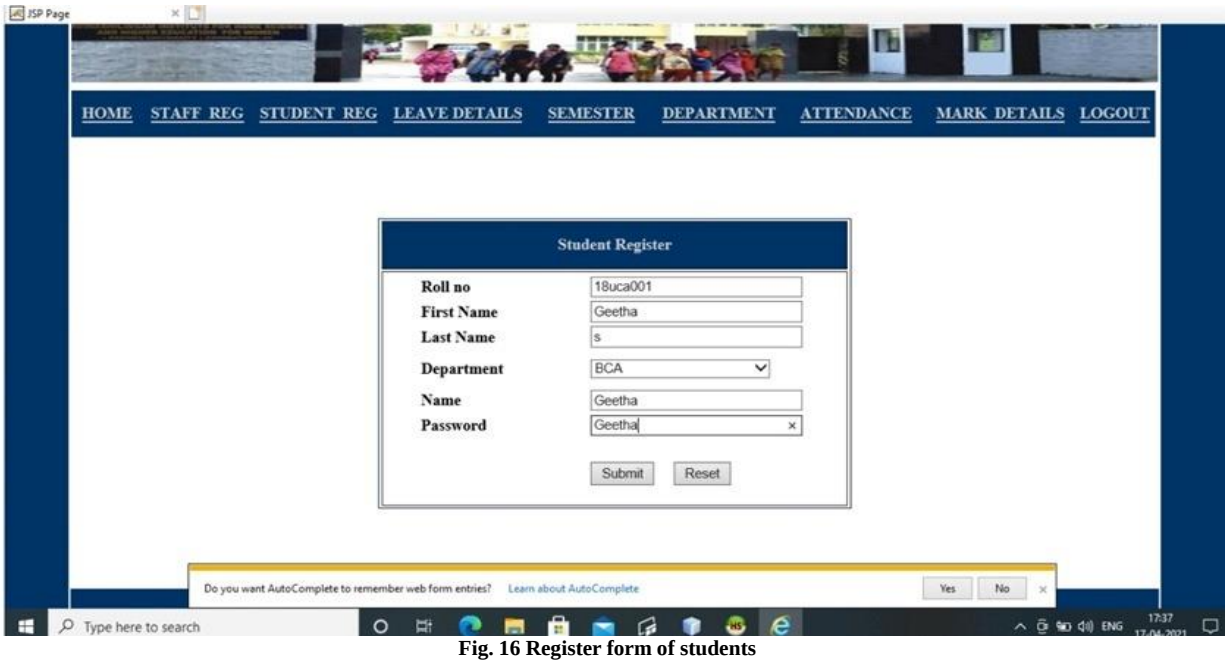

Fig. 16 Register form of students

Figure 15 represents the staff registration interface where the admin is provided a form to enter the staff details, such as name, employee number, and their department. The admin is then able to securely add new faculty members to the academic management system.

The records submitted are protected using AES-256 for encryption, and the records are stored on the Blockchain ledger, where they are immutable for verification purposes.

Figure 16 depicts the student registration screen, where students enter their roll number, name, department, and password in order to create a student profile by encrypting the content of student registrations with AES-256 and storing it in a Blockchain ledger to allow for new students' secure enrollment in the academic management system. Additionally, this process provides assurance that each student's registration is authentic and that unauthorized changes have not been made to that student's registration.

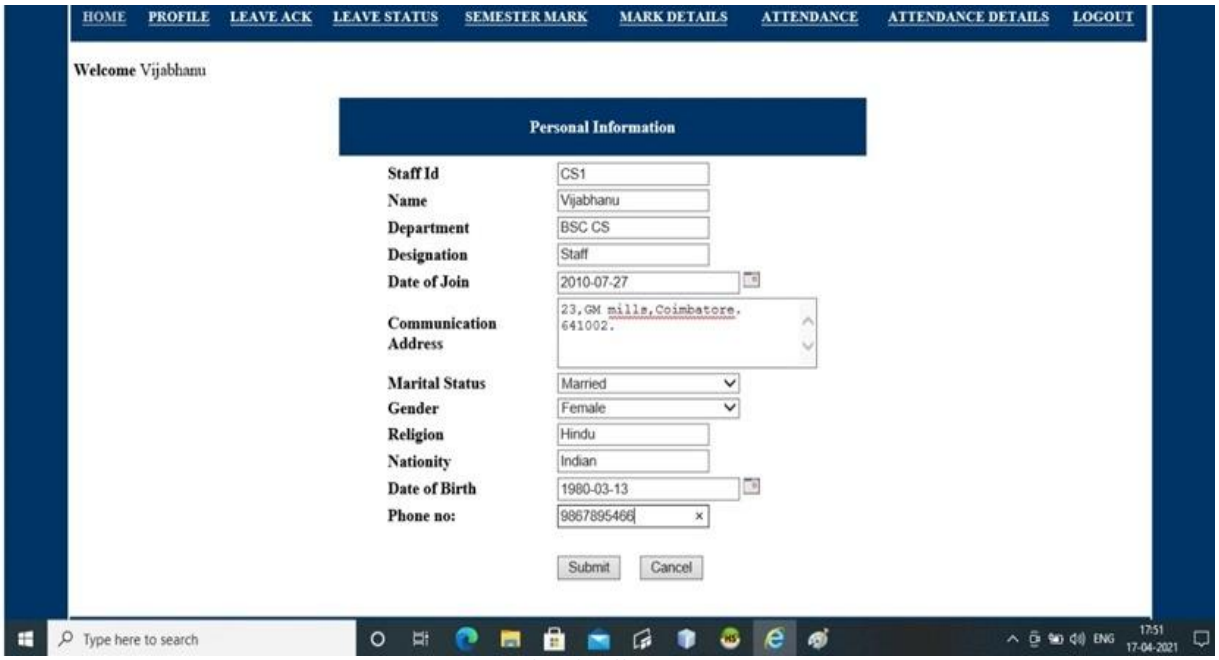

Fig. 17 Profile of staff personal details

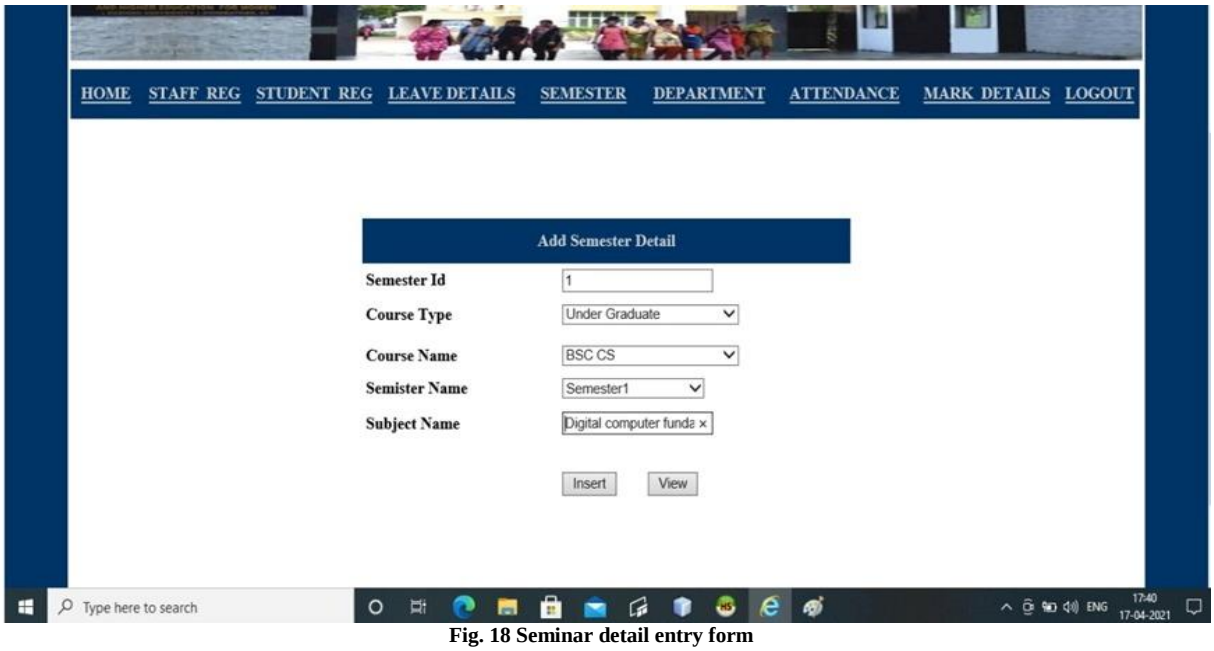

Fig. 18 Seminar detail entry form

The information screen for staff members' personal details is shown in Figure 17. Here, staff members can update their name, designation, department, contact information (including email address and phone numbers), and demographic information. This module guarantees the accurate maintenance of staff records in the system. All data is encrypted and audited using a Blockchain network, ensuring data integrity and transparency.

Figure 18 represents the semester detail entry form, where the admin inputs the semester ID, course type, course name, semester name, and subject details. This function organizes documentation of academic details for each program properly. The written data is encrypted with AES-256 and stored in the Blockchain ledger to ensure accuracy and prevent unauthorized modifications.

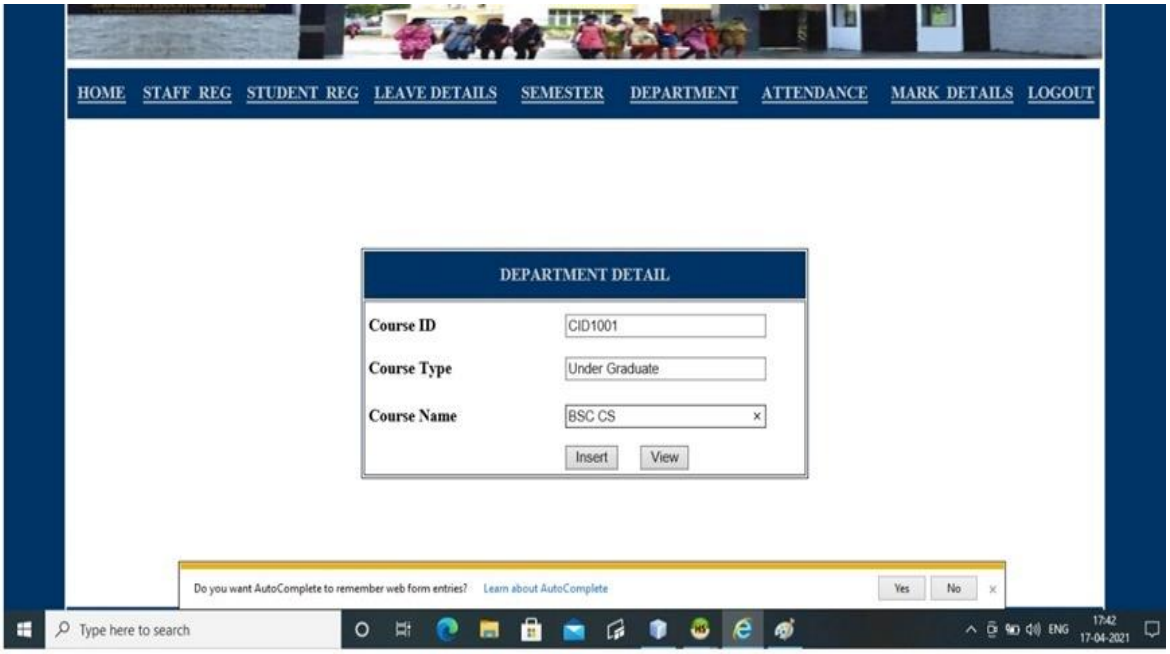

Fig. 19 Department detail entry form

Figure 19 represents the department detail entry form, where the admin enters the course ID, course type, and course name. This function enhances academic management functionality, provisioned at the department level. All departmental data is secured using AES-256, and data is stored in the Blockchain ledger. This module supports streamlined academic management by organizing department-level records and information.

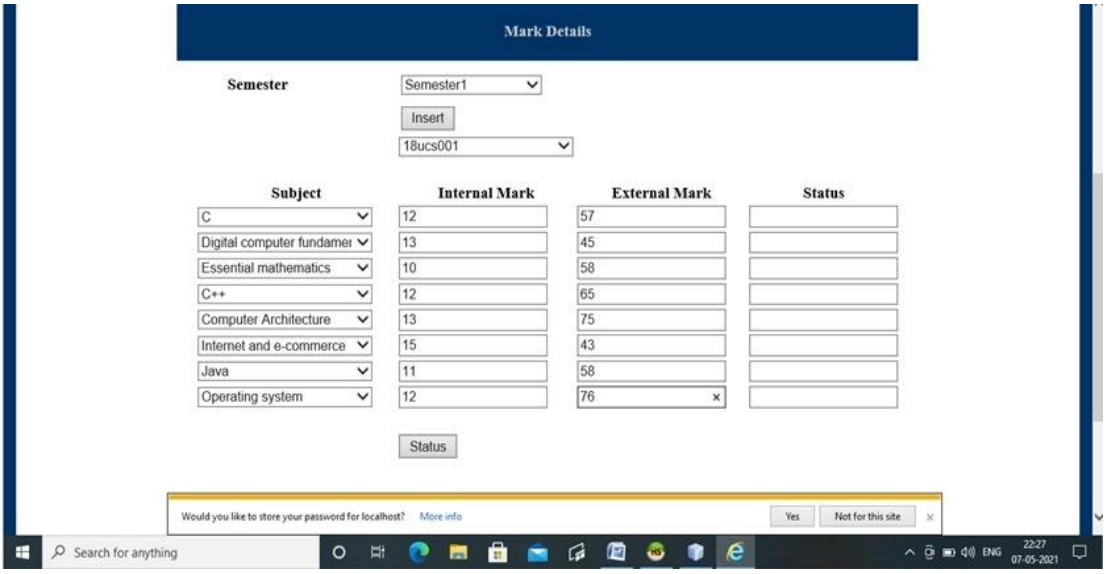

Fig. 20 Students mark the entry page

Figure 20 represents the marks entry page, where staff enter the internal and external marks for students' subjects. This feature is developed so that all entries of data of the students' academic performance are entered accurately. All records are encrypted and stored in the Blockchain ledger, while the DL models have access to all data to predict students' performances.

Figure 21 shows the mark status page, which shows students' marks compiled for the subject. It shows internal marks, external marks, and total marks with a performance status. The documenting of marks is analyzed with DL algorithms, yielding early performance indicators.

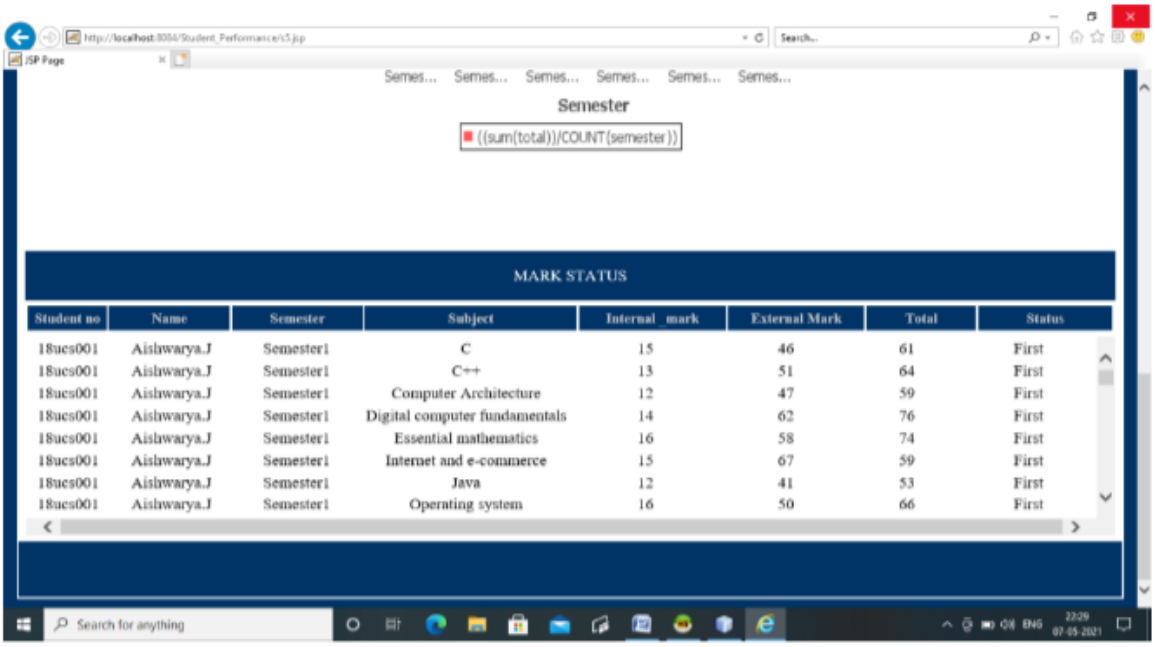

Fig. 21 Mark status page

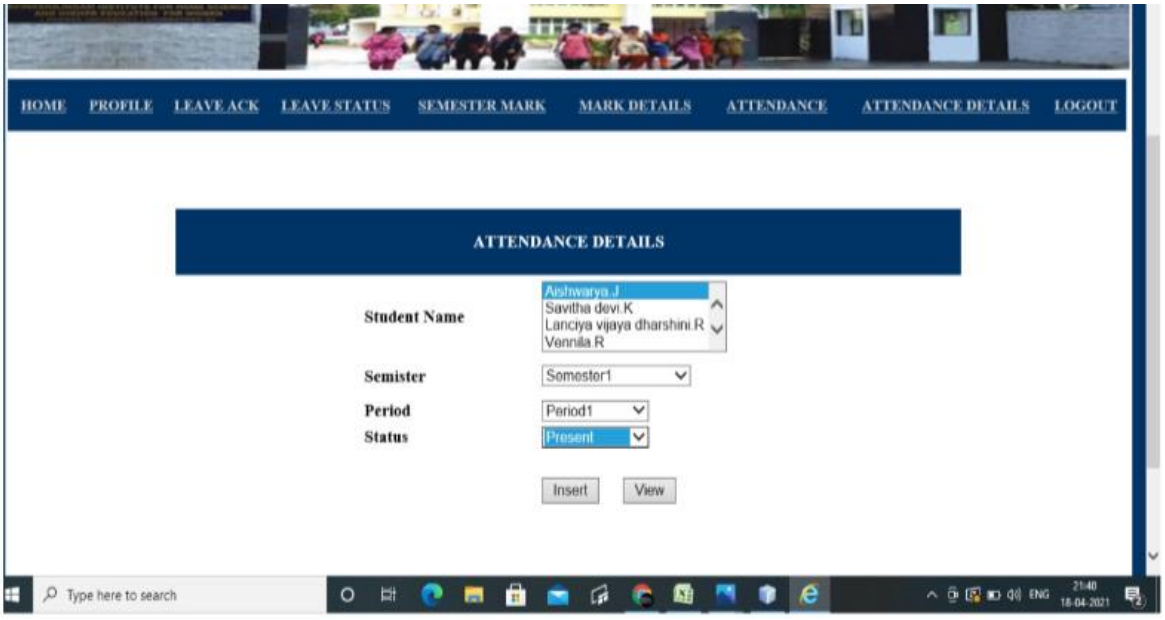

Fig. 22 Attendance details entry form

Figure 22 shows the attendance detail entry form, allowing staff to modify the attendance of the students by selecting the semester, subject, and period. Attendance is essential to monitor the students' academic participation. The decoded attendance data is secured with AES-256 encryption and analyzed using DL models, exposing at-risk students.

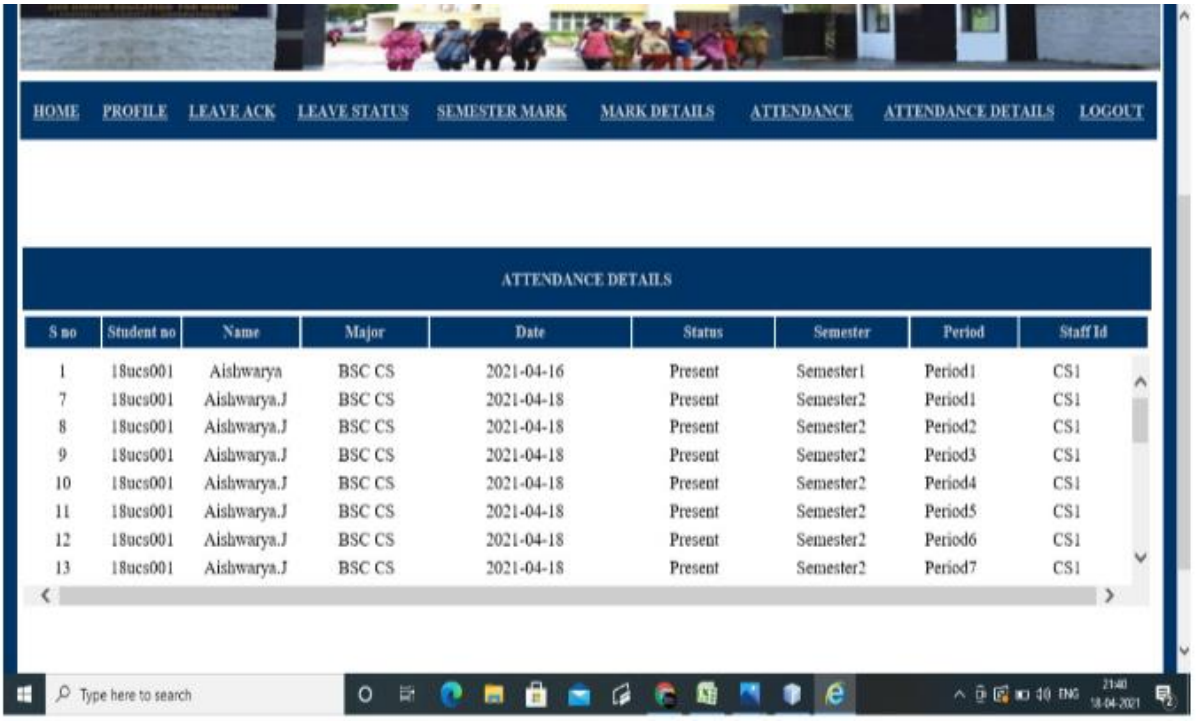

Fig. 23 Attendance status page

Figure 23 illustrates the attendance record list, presenting student names, roll numbers, dates, and presence/absence status. The attendance record list helps faculty to view student attendance/missing patterns comprehensively. The attendance record is stored in the Blockchain permanently and can never be modified. Faculty are reporting attendance patterns on Blockchain to be transparently processed.

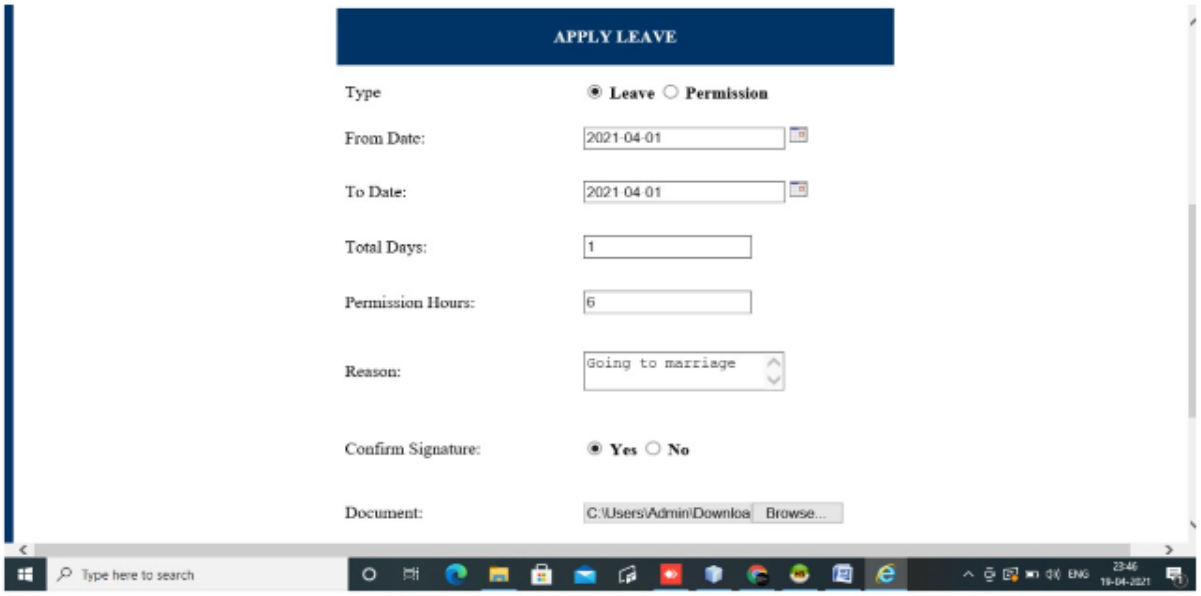

Fig. 24 Student leave application form

Figure 24 illustrates the student leave application form, through which students apply for leave by specifying their application dates, the reason for leave, and providing supporting documentation. There are options for the application to be approved electronically and securely. Leave requests are saved in the Blockchain ledger and traced if needed, and the student leave applications are protected using AES-256 encryption.

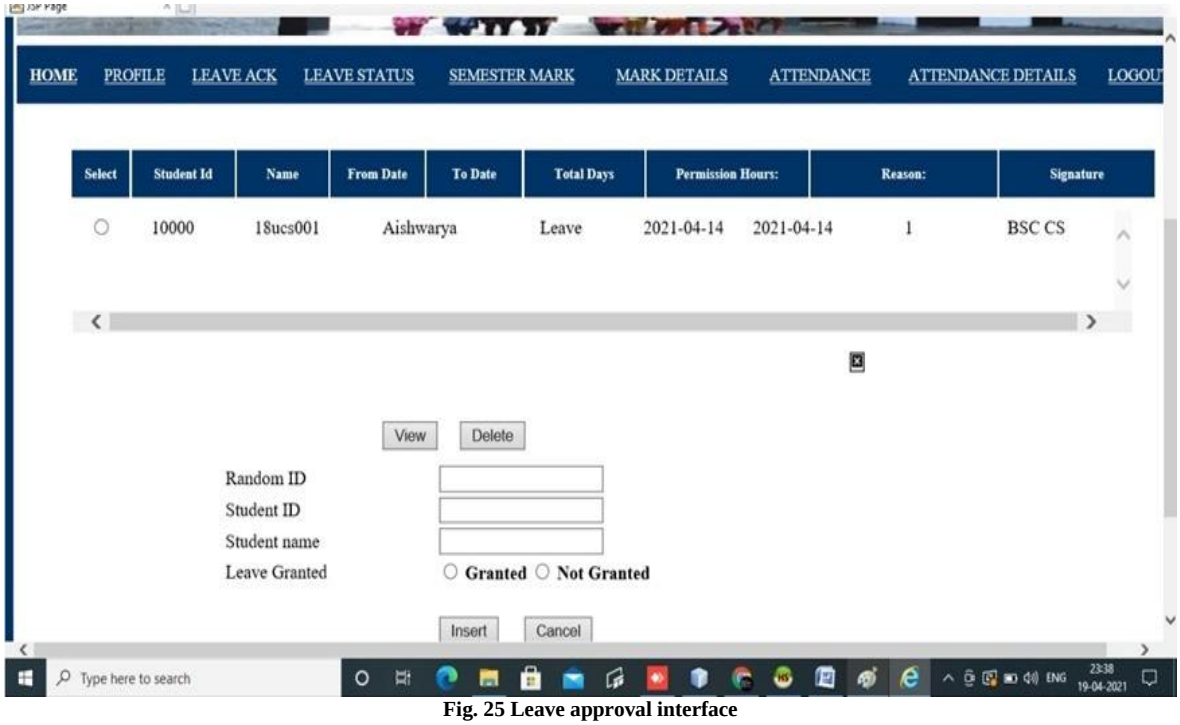

Fig. 25 Leave approval interface

Figure 25 represents the leave approval interface where staff members examine the leave application submitted by a student through the student ID, student name, date requested, reason for leave, and total days. It allows the administrator or staff member to approve or deny the leave request securely. This is recorded using the Blockchain ledger for integrity purposes, while the communications are encrypted using AES-256 encryption.

Fig. 26 Mark analysis chart

Figure 26 shows the marks analysis chart showing student performance in semesters in a bar chart. The chart output shows how to interpret whether the students have improved or not. The DL improves the chart analysis by forecasting future academic performance using historical data.

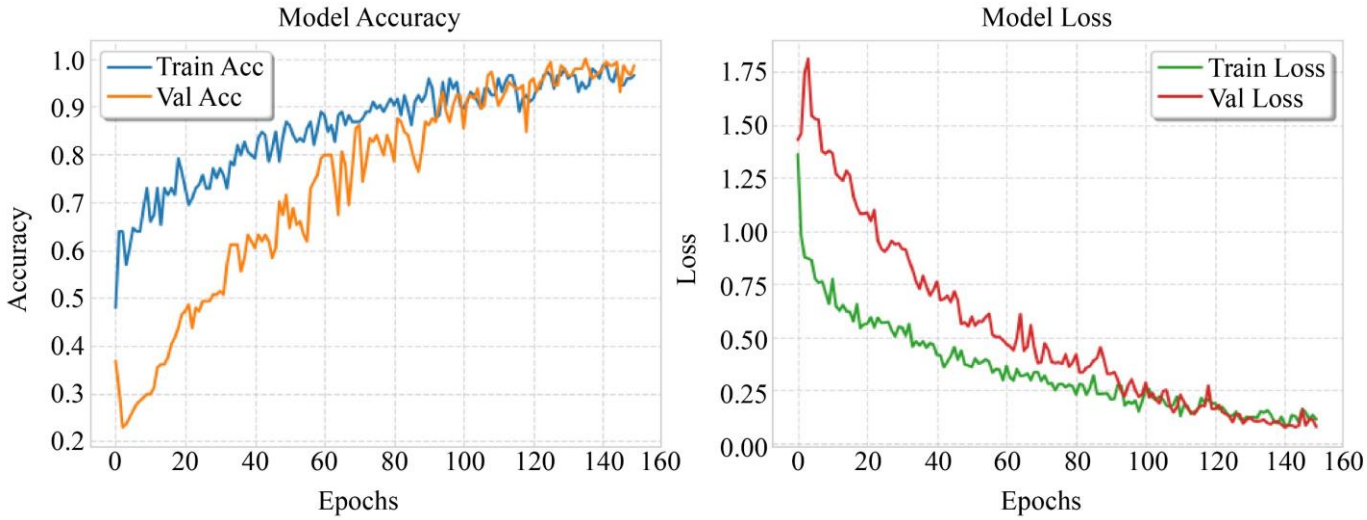

Fig. 27 Model accuracy and model loss

Figure 27 shows the training and validation performance of the classification model with 150 epochs. The accuracy curve shows that the training accuracy gradually improved and eventually approached 98%, and validation accuracy also follows a similar trend and is grouped at 98.6%. This shows that the model is learning effectively and generalizing well. The loss curve supports both training and validation loss values that constantly reduce and converge to 0.1, which shows less error in classification and stable optimization of the model.

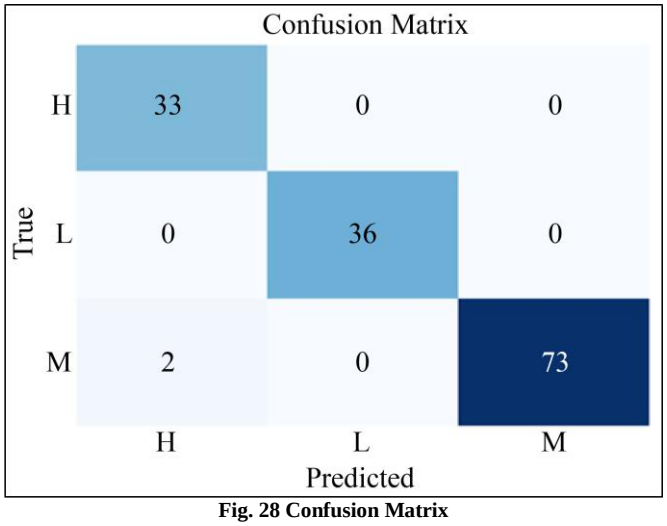

Fig. 28 Confusion Matrix

Figure 28 provides a confusion matrix to evaluate the classification results on the test set. The model accurately classified all instances of the Low (L) class, with only two Medium (M) class samples being confused with High (H). The classification success rates between the High, Low, and Medium categories are of concern; there are no significant instances of misclassification. This result confirms the reliability and precision of the model.

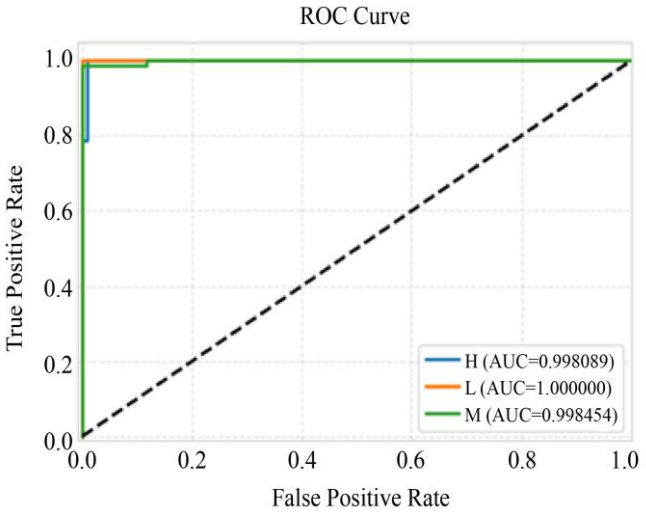

Fig. 29 ROC curve

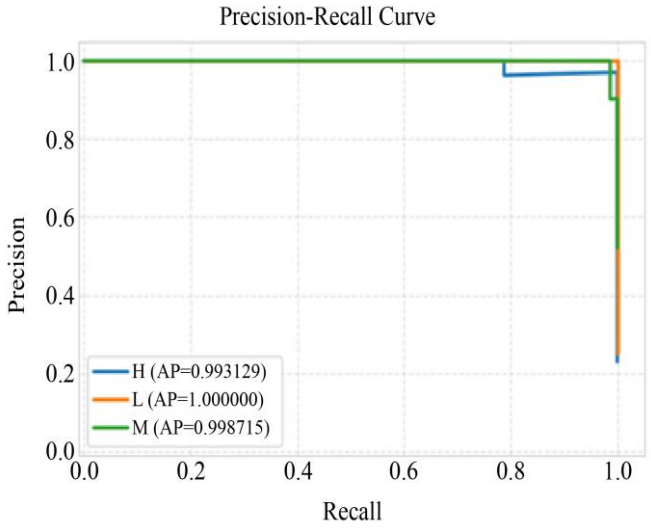

Fig. 30 Precision- Recall curve

Figure 29 presents ROC curves for the three classes. The curves confirm the model's strong discriminative ability. The corresponding Area Under the Curve (AUC) values are also very high: 0.9981 for High, 1.0 for Low, and 0.9985 for Medium. These results indicate perfect class separability, meaning the model is confidently distinguishing between the categories.

Figure 30 depicts Precision-Recall (PR) curves for the three classes. The curves consistently remain very near the maximum precision and recall point, which indicates excellent predictive performance. The Average Precision (AP) scores for High, Low, and Medium are 0.9931, 1.0000, and 0.9987, respectively, confirming that the model has nearly achieved an ideal situation between precision and recall.

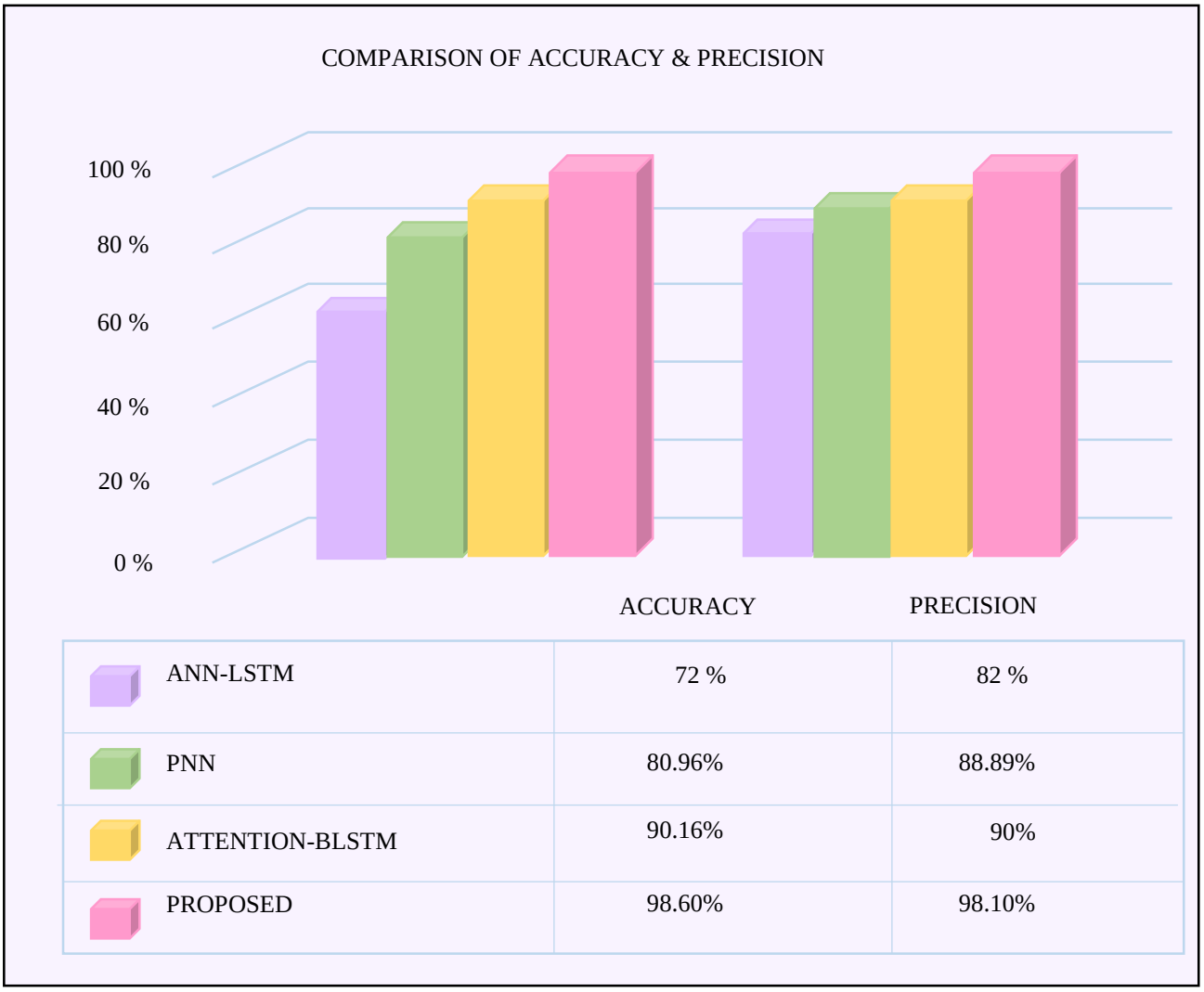

Fig. 31 Comparison of DL performance metrics

Table 1. Evaluation of recall and F1-score

DL methods	Recall	F1-score
ANN-LSTM	58%	68%
PNN	92.23%	82.87%
ATTENTION-BILSTM	90%	90%
PROPOSED	99%	98.5%

Figure 31 shows the accuracy and precision for ANN-LSTM [15], Probabilistic Neural Network (PNN) [16], Attention-BiLSTM [17], and the proposed model. The proposed model shows better results with 98.6% accuracy and 98.1% precision. The proposed model exhibits the best overall metrics compared to the others in this study.

Table 1 represents recall and F1-score for ANN-LSTM [15], PNN [16], Attention-BiLSTM [17], and the proposed model. The proposed model shows better results with 99% of recall and 98.5% of F1-score compared to other listed methods.

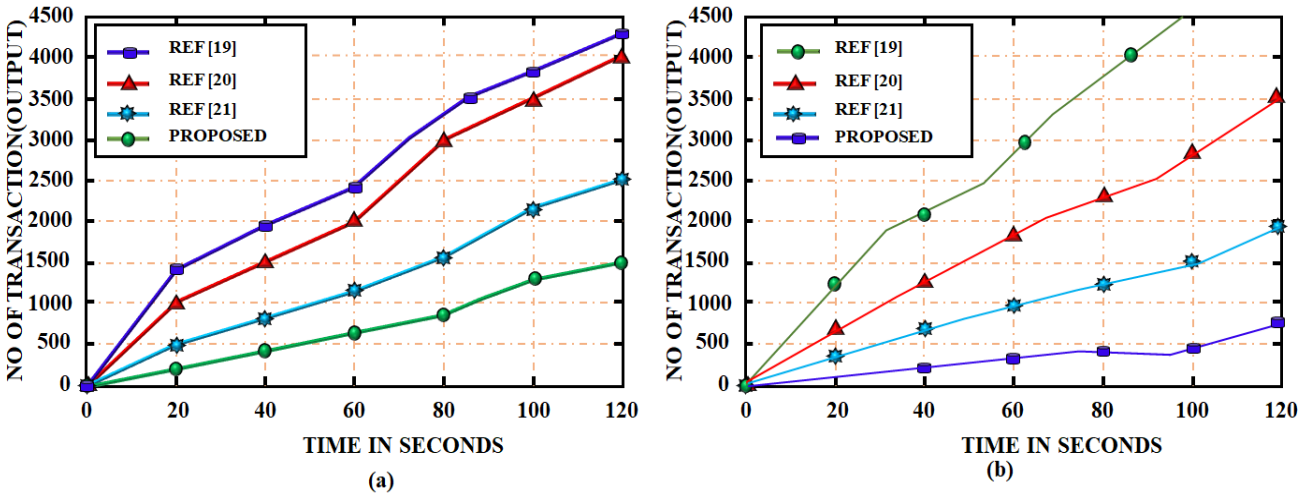

Fig. 32 Comparison of (a) Validation time, and (b) Throughput.

Figure 32 presents the comparison of validation time and throughput, demonstrating the performance dynamics of the presented hybrid AES-256 with a blockchain framework for authenticating academic certificates. Figure 32 (a) compares the validation time of four approaches with the proposed model over the period of 120 seconds. The method proposed in this work is slightly more validatory in latency than in the conventional approaches; the additional AES-256 cryptographic algorithm remains responsive enough to provide secure and tamper-evident validation. Figure 32 (b) shows throughput analysis, with the number of transactions validated over time. In this case, the proposed approach surpasses all references with higher scalability and efficiency.

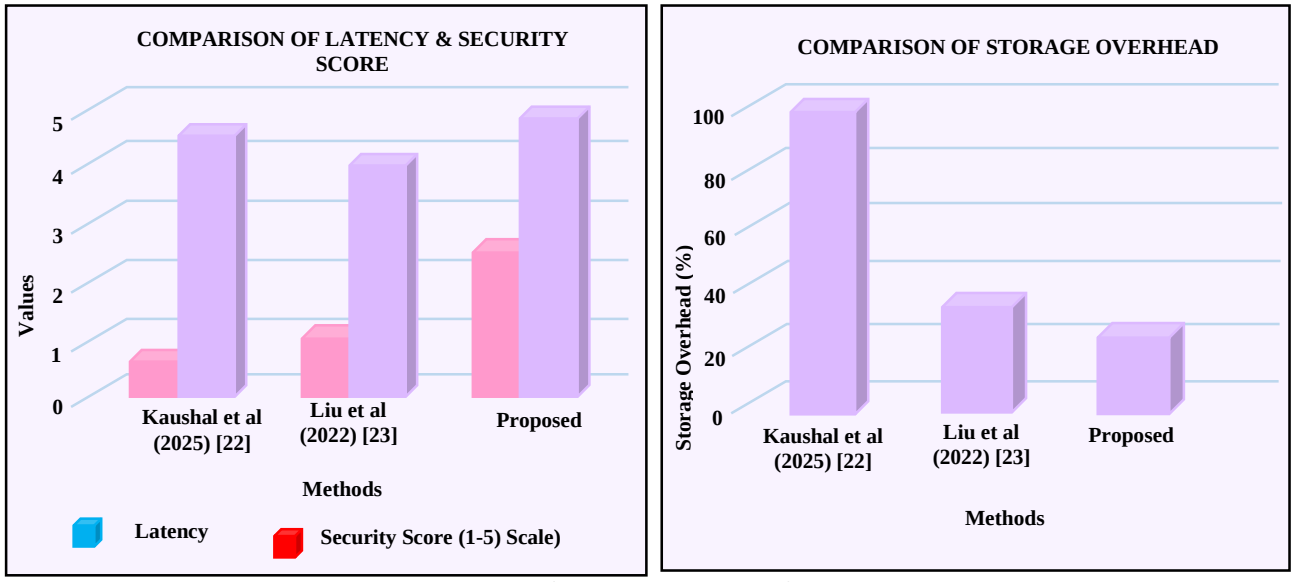

Fig. 33 Comparison of AES 256-blockchain performance metrics

Figure 33 represents an overview of a comparative study of AES 256-blockchain performance measures: latency, security, and storage overhead across existing methods [20], [21] and the proposed framework. Latency denotes the amount of time it takes to validate a transaction, with lower values being more desirable. Security indicates the protection against attacks or modifications, with higher values being more desirable. Storage Overhead indicates the memory necessary to keep records on the blockchain, with lower values being more scalable. Based on the comparisons above, the proposed framework provides the best general balance by achieving higher security and lower storage overhead while maintaining appropriate latency, thus estimated to be more efficient and secure for the use case of academic credential verification and fraud prevention.

4.1. Discussion and Comparison with Existing Methods

The proposed CARTNet framework outperforms ANN-LSTM, PNN, and Attention-BiLSTM, as shown in the above results. This improvement is essentially due to the incorporation of chaotic attractor-based feature modeling, multi-head attention, recurrent learning, and transformer encoding, which work together to capture complex, nonlinear, and temporal patterns in student data more effectively than traditional models. The combination of AES-256 encryption technology along with the benefits of using blockchain allows for secure and unalterable data storage, thus reducing the risk of having data stored on a centralized platform and improving the overall reliability of the system.

5. Conclusion

This research investigates the blockchain-enabled model of secure academic credential certificate management, which aims to offer a holistic resolution to the issues associated with forgery and modification of certificates in a centralized manner. The model is constructed with a decentralised database to deliver immutable and verifiable information relating to the credential, and by using smart contracts, it provides for the automatic issuance, validation, and archival of credentials. The implementation of a Java-based integration allows for enhanced flexibility in the use of existing solutions. The innovative aspect of this model includes DL-based CARTNet integration, enhanced predictive capabilities for the assessment of future academic performance. With performance validation from a Python software indicating accuracy of 98.6%, precision of 98.1%, recall of 99.1% and FI-score of 98.5% confirming both data integrity and predictive capabilities.

The evaluation of AES 256 blockchain performance measures, including latency, throughput, verification time, security, and storage overhead, demonstrates that the proposed framework provides superior efficiency, scalability, and reliability for academic certificate verification and fraud prevention. By merging the cryptographic security layer with automation, the model represents a scalable solution to the long-standing problems of digital certificate verification and support for educational decision-making.

References

[1] Guiyun Feng, Muwei Fan, and Yu Chen, "Analysis and Prediction of Students' Academic Performance Based on Educational Data Mining," *IEEE Access* vol. 10, pp. 19558-19571, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Adnan et al., "Predicting at-Risk Students at Different Percentages of Course Length for Early Intervention Using Machine Learning Models," *IEEE Access*, vol. 9, pp. 7519-7539, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Aya Nabil, Mohammed Seyam, and Ahmed Abou-Elfetouh, "Prediction of Students' Academic Performance Based on Courses' Grades Using Deep Neural Networks," *IEEE Access*, vol. 9, pp. 140731-140746, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Arun Kumar Soma, "Enhancing Supply Chain Transparency and Integrity: A Permissioned Blockchain Framework," *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, Bhubaneswar, India, pp. 819-826, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Arun Kumar Soma, "Hybrid RNN-GRU-LSTM Model for Accurate Detection of DDoS Attacks on IDS Dataset," *Journal of Modern Technology*, vol. 2, no. 1, pp. 283-291, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] R. Udayakumar et al., "Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification," *Journal of Internet Services and Information Security*, vol. 13, no. 4, pp. 138-157, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Seong-Kyu Kim, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm," *Electronics*, vol. 11, no. 14, pp. 1-32, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Suyel Namasudra et al., "Blockchain-Based Medical Certificate Generation and Verification for IoT-Based Healthcare Systems," *IEEE Consumer Electronics Magazine*, vol. 12, no. 2, pp. 83-93, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Qiang Tang, "Towards Using Blockchain Technology to Prevent Diploma Fraud," *IEEE Access*, vol. 9, pp. 168678-168688, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Qilin Zhou et al., "CrossCert: A Cross-Checking Detection Approach to Patch Robustness Certification for Deep Learning Models," *Proceedings of the ACM on Software Engineering*, vol. 1, no. FSE, pp. 2725-2746, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Muhammad Nauman et al., "Guaranteeing Correctness of Machine Learning Based Decision Making at Higher Educational Institutions," *IEEE Access*, vol. 9, pp. 92864-92880, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Dhruvil Shah et al., "Integrating Machine Learning and Blockchain to Develop a System to Veto the Forgeries and Provide Efficient Results in Education Sector," *Visual Computing for Industry, Biomedicine, and Art*, vol. 4, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mirna Nachouki et al., "Student Course Grade Prediction using the Random Forest Algorithm: Analysis of Predictors' Importance," *Trends in Neuroscience and Education*, vol. 33, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Zaffar Ahmed Shaikh et al., "Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture," *Applied Sciences*, vol. 12, no. 5, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fatima Ahmed Al-azazia, and Mossa Ghurab, "ANN-LSTM: A Deep Learning Model for Early Student Performance Prediction in MOOC," *Heliyon*, vol. 9, no. 4, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Rosa Leonor Ulloa Cazarez, "Accuracy Comparison between Statistical and Computational Classifiers Applied for Predicting Student Performance in Online Higher Education," *Education and Information Technologies*, vol. 27, pp. 11565-11590, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Bashir Khan Yousafzai et al., "Student-Performulator: Student Academic Performance Using Hybrid Deep Neural Network," *Sustainability*, vol. 13, no. 17, pp. 1-21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] R. Manoj, and Sandeep Joshi, "Securing Academic Certificate Verification with Blockchain-based Algorithmic Rules," *2023 IEEE 4th International Multidisciplinary Conference on Engineering Technology (IMCET)*, Beirut, Lebanon, pp. 242-247, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Rojalina Priyadarshini et al., "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," *IEEE Access*, vol. 13, pp. 27037-27049, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Rajesh Kumar Kaushal et al., "Hyperledger Fabric based Remote Patient Monitoring Solution and Performance Evaluation," *Peer-to-Peer Networking and Applications*, vol. 18, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Wenxuan Liu et al, "Ring-Overlap: A Storage Scaling Mechanism for Hyperledger Fabric," *Applied Sciences*, vol. 12, no. 19, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]