Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.2, 2025, pp.28-37

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.2.05

# Blockchain for Library Records Management: A Secure and Decentralized Approach

**Shweta Sharma[1*], Dr.L. Lakshmanan[2], Dr. Prabhat Kumar Sahu[3], Dr. Trapty Agarwal[4] and M.R. Tejeshwari[5]**

[1*]Research Scholar, Centre for Research Impact and Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India

[2]Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

[3]Associate Professor, Department of Computer Science and Information Technology, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India

[4]Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India

[5]Assistant Librarian, Learning Resource Centre, JAIN (Deemed to be University), Bangalore, Karnataka, India

Email: [1]shweta.1015@chitkara.edu.in, [2]lakshmanan.cse@sathyabama.ac.in, [3]prabhatsahu@soa.ac.in, [4]trapty@muit.in, [5]tejeshwari.m.r@gmail.com

ORCID: [1]https://orcid.org/0009-0006-4008-6402, [2]https://orcid.org/0000-0001-8987-5724, [3]https://orcid.org/0000-0002-0460-9783, [4]https://orcid.org/0009-0007-4081-4999, [5]https://orcid.org/0009-0009-2130-4840

(Received 12 February 2025; Revised 26 March 2025, Accepted 07 April 2025; Available online 25 June 2025)

*Abstract* - **Aim: In recent times, growths in digital infrastructure have led to the rapid expansion of Electronic Library Records (ELRs). An active Library Records Management (LRM) information system allows data owners', students, faculty, and staff, to achieve and strongly share their data with chosen entities. However, the rising volume of ELRs poses challenges in ensuring data security, access control, and efficient resource usage.**

**Methods: To address these difficulties, this research presents a novel Blockchain Enabled Secure Library Records Management (BESLRM) with a Deep Learning (DL) model. The construction allows library administrators to read and update records safely, gives users-controlled access privileges, and facilitates automated alerts for overdue returns or the accessibility of reserved books. For data encryption, the Advanced Encryption Standard (AES) is employed, while the Efficient Transient Search Optimization Algorithm (ETSO) is used to produce optimal encryption keys, enhancing the AES performance. Library data is collected from user logs, and borrow records. Preprocessing involves cleaning, encoding, and normalization. Block chain records user actions like reservations, returns, and book check-outs, and it is used to store and trade library data. Digital resources or external data are safely connected to external storage. An Efficient Transient Search-driven Conditional Variational Autoencoder (ETS-CVAE) is used to forecast user preferences, identify unusual usage patterns, and optimize inventory after decryption at the authorized end.**

**Results: The suggested approach exhibits better performance, which includes a recall of 96.50%, accuracy of 98%, F1-score of 95.89%, precision of 94%, and Kappa score of 93%.**

**Conclusion: Experimental conclusions confirm that the proposed model confirms superior safety, transparency, and efficiency compared to traditional LRM approaches.**

*Keywords* - **Library Records Management (LRM), Advanced Encryption Standard (AES), Efficient Transient Search-driven Conditional Variational Autoencoder (ETS-CVAE), Library Data, Blockchain, Security, Information System.**

## I. INTRODUCTION

Libraries have evolved from being a repository of knowledge to a hub of information and knowledge. With advancements in technology, libraries are being transformed by Artificial Intelligence (AI), which is transforming the preservation of information and user services. AI is transforming library computerization, improving information discovery, and enhancing user experiences, thus transforming library operations (Okunlaya et al., 2022). Library management systems are crucial for organizing and retrieving library collections, but traditional centralized arrangements are vulnerable to security breaches. Library Management Systems (LMS) are software applications considered to modernize library operations, and automate tasks like cataloging, movement, acquisitions, patron management, and reporting, providing a centralized platform for librarians and staff to improve consumer knowledge's and modernize processes (Puzier & Nous, 2022; Farhang & Rashidi, 2015). The modern library indicates improving library services through the application of advanced knowledge like big data, Internet of Things (IoT), and cloud computing AI. These developments allow libraries to transform from passive to

active offerings (Kim, 2024). Blockchain technology, with its essential properties of decentralization, non-tampering, transparency, security, and reliability, has the potential to dramatically improve the public cultural services market (Meng et al., 2025). As blockchain technology has developed, many businesses have noticed and several big businesses have contracted for research and development regarding its usage across several industries. Various libraries around the world are buying and accepting resources in multiple currencies, potentially affecting book budgets (Al-Farsi et al., 2021). Libraries employ blockchain to safeguard user and resource data, create an adaptive library services model, and enable intelligent communication and management among consumers. This provides security of data and dependability, as well as the efficiency of borrowing and returning books, and protects users' private information (Prakash & Prakash, 2023). The use of technology in library functions has the intention of empowering users and improving library services (Ajani et al., 2022). Libraries have adopted blockchain technology to support information sharing and archiving, access to and acquisition of resources, protection of resources, and user data privacy and security (Khan et al., 2024; Chinnasamy, 2024). The technology also advances metadata systems, allowing secure distribution and digital first-selling rights. It can speed library development while lowering administrative expenses by mechanizing agreements between libraries and vendors for services like inter-library offering and service subscriptions. Centralized library systems are susceptible to data breaches, manipulation, and individual points of failures. They lack transparency, real-time organization, and consistent traceability. Ensuring data integrity and safe accessibility across many branches remains a substantial problem. To overcome the challenges, this research generates a Block chain-Enabled Secure Library Records Management (BESLRM) system to advance security and efficiency in data management. It needs to provide safe, decentralized security, automatic signals, and preference estimates to library users (Almolhis, 2024).

The organization of the research is given as follows: Section 2 explains the related articles. Section 3 illustrates the methodology and Section 4 determines the results and discussion. Section 5 examines the conclusion of the research.

## II. Related Works

This section offers an overview of the literature, organized by references, objectives, methods, and limitations, providing a brief summary of the research.

Fasola et al., (2024) examined the awareness, willingness, and capability of Nigerian university librarians to use blockchain for library service offerings. A questionnaire had been conducted with 105 librarians from 38 higher education institutes. The assumptions revealed a strong correlation among librarians' knowledge and understanding of blockchain and their willingness to employ it. However, issues such as technophobia, a requirement of information, scientific transportation, unpredictable energy supply, and inadequate internet access can hinder the request of blockchain system in Nigerian libraries. Ashtagi et al., (2024) discovered the possibilities of blockchain methodology to change how libraries function, and make library functions more secure, achievable, and effective. The blockchain's instinctive log creation provided a secure method to trace and check operations and maintain information integrity free from unauthorized modification. The blockchain allowed libraries to accomplish things like book sharing, book returns, and expenditure organization with fewer person actions and executive mistakes (Alhassan et al., 2024).

The Technology Organization and Environment theory (TOE) and combined Technology Acceptance Model (TAM) system were applied by (Akintunde & Amuda, 2024) to predict academic libraries' success in adopting blockchain technology. A combination of librarians and system analysts was used to collect information from 338 participants. The outcomes exposed that perceived usefulness and policy were important factors in determining library adoption purposes. Blockchain provided unrestricted accessibility to resources, secured user information, and facilitated partnerships between users and library staff. Infrastructure expenses, issues with security, and librarians' inadequate conception of blockchain technology were all challenges. The responsiveness and observation of blockchain system in library and records administration, with an emphasis on the fourth industrial revolution, was examined (Tella et al., 2022). The research included ten system librarians and ten archivists from five separate libraries and archives. Research findings indicated that both libraries and archives were conversant with the concept of blockchain, which serves to store information in cooperative settings and assists archives in producing distinctive, reliable records. Nevertheless, confronts like completion, maintenance expenses, and sustainability concerns were discovered.

The utilization of blockchain system for personality organization in telecom examinations was determined by Manda, (2024). It highlighted its decentralized model, enhancing security, transparency, and user control. The permanent blockchain database reduced data theft and corruption risks. Intelligent agreements mechanize individuality authentication procedures, decreasing dependence on central systems. Manakhari & Jadhav (2024) suggested that telecom companies can create a secure identity management framework by collaborating and using innovative methods. The Inter Planetary File System (IPFS), a collaborative hyper-media procedure, provided an alternative to standard federal cloud storage by decentralizing digital content storage and organization. The research explored IPFS's security features, including content-addressable retention, encrypted hash linkage, and distributed architecture, demonstrating that decentralized methods had moderate safety effects (Zhang et al., 2024).

Federated Learning allows Machine Learning (ML) models to be trained across multiple companies without sharing

proprietary data, as stated by (Verma, 2025). Standard federated learning has issues because the data was distributed identically rather than separately. A hierarchical federated learning system based on blockchain methodology was demonstrated to strengthen the preparation of non-IID information, safeguard the security and privacy of information, and boost effectiveness. The approach employed blockchain architecture to eliminate non-IID local data while increasing the accuracy of models. Smart contracts were employed for distribution and collection, while a main blockchain was intended for local simulation preservation and federation aggregate.

### A. *Research Gap*

Library record management yet relies on centralized systems, which are prone to data breaches, manipulation, and system failures. Although blockchain offers promising features like decentralization, transparency, and security, its application in library systems remains under-researched. There is a lack of comprehensive analyses exploring its feasibility, implementation challenges, and impact on data integrity in library environments.

## III. METHODOLOGY

This research improves library record management and provides a systematic approach that combines safe encryption, intelligent modeling, and optimal search strategies. The research utilizes Kaggle's Library Transaction Dataset, which has been cleaned and lemmatized to ensure correctness. A CVAE strategy, boosted with Efficient Transient Search (ETS), predicts user preferences and detects abnormal actions. For the protection, AES encryption is utilized, with ETS optimizing key generation to employ the electrical circuit-inspired dynamics. Fig. 1 depicts the overview of the methodology flow.

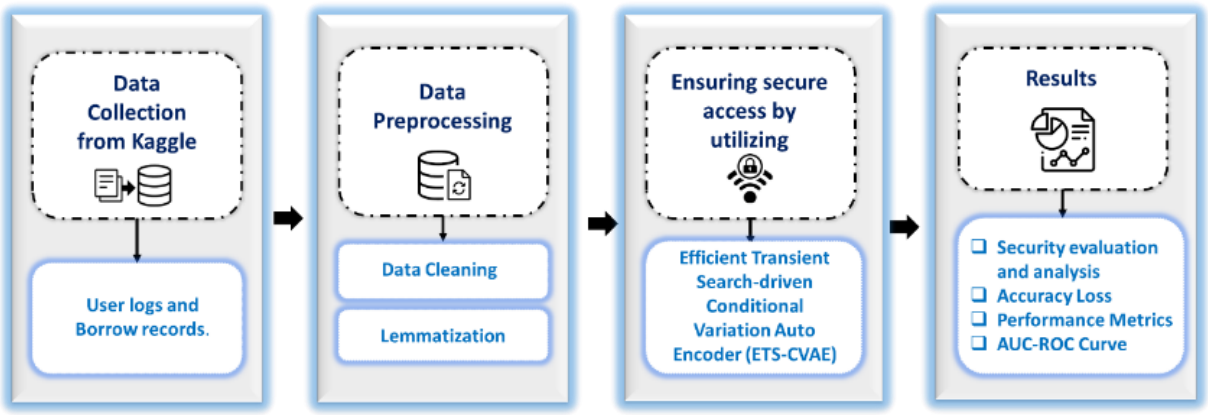


Fig. 1 Overview of the Methodology

### A. *Data Collection*

This research gathers dataset (https://www.kaggle.com/datasets/ziya07/library-transaction-dataset/data) from Kaggle. The Library Transaction Dataset is evaluated to analyzes and predict library book borrowing behaviors, with an emphasis on difficult forecasts. It contains the detailed records of user interactions with the library system, including the borrowing and return of books, reservations, and consumption trends.

### B. *Data Preprocessing*

The data is preprocessed in two phases: data cleaning and lemmatization. These processes enhance the accuracy of data and organization, preparing it for subsequent development and evaluation.

### C. *Data Cleaning*

Data cleaning, an essential component of data preparation detects and eliminates imperfect, incomplete, inaccurate, or unnecessary data elements, allowing for replacement, modification, or deletion. It involves adjusting missing values, removing duplicate rows, or removing unwanted columns. Missing values or missing data are features or observations where values are not stored and must be filled or removed.

### D. *Lemmatization*

Following the data cleaning, lemmatization is performed. Lemmatization is the process of eliminating or replacing a word's suffix to return it to its bottom, known as a lemma. Lemmatization is a frequent text preparation step in Natural Language Processing (NLP) that has demonstrated to produce better outcomes.

### E. *Ensuring Secure Access by Utilizing an Efficient Transient Search-driven Conditional Variational Autoencoder (ETS-CVAE)*

ETS-CVAE is a framework that predicts user preferences based on previous borrow records and access logs, enabling personalized recommendations and automated alarms. It also detects irregular usage behaviors, which improves system safeguard and information authenticity, such as abnormal borrowing behavior or potential unwanted access. The BESLRM system protects critical library data with the Advanced Encryption Standard (AES). AES encrypts ELRs,

such as user logs, borrows records, and transaction activity, before they are maintained or communicated over the blockchain. The integration of ETS-CVAE into the BESLRM system advances efficiency and accessibility by offering various advantages.

### *F. Conditional Variational Autoencoder (CVAE)*

External control is the method used to create VAE information. VAE is composed of two feed-forward networks: one encoder and one decoder. The encoder translates an effort X into a concealed break illustration p, which is subsequently decoded and returned to the interplanetary substances A′. CVAE is a valuable instrument for intelligent data examination and individualized service distribution. It examines user interactions, predicts preferences, and develops conditional distributions to identify odd usage patterns, so improving system security and resource allocation by detecting anomalies or exploitation. The CVAE enables users to create an innovative outcome that remains similar to the original database. CVAE is an advanced procreative model that enhances VAE by assigning labels to the encoder and decoder. To achieve the preferred outcome, this approach transmits the consequence to the decoder along with the vector from the hidden state that is chosen from the conventional sharing. Assume a particular end is utilized to produce two separate integers. In this instance, it performs properly as the CVAE is no longer reliant on the hidden area vector p and instead focuses on the tag, allowing it to process the data efficiently, as determined in Equation (1).

$$D[\log M(A|p,c)] - WQP[Z(p|A,c)||M(p|c)]$$

$$D[\log M(A|p,c)] - WQP[Z(p|A,c)||M(p|c)] \quad (1)$$

Here $Z(p|A,c) and\ and\ M(p|c)$ are the probability allocations of the hidden state. $WQP$is defined as follows $WQP\big[Y(\mu(A,c),\Sigma A,c)\big)||Y(0,1)] = 1/2\Sigma r(\exp\big(\Sigma(A,c)\big) + \mu 2(A,c) - 1 - \Sigma(A,c)), where\ \mu(A,c)$ represents the average and $\Sigma(A,c)$ denotes the covariance and situation; $exp$ represents the promoter role; $Z(p|A,c)$ represents the encoder that is used to compute the average and the SD for the effort and situation; $M(p|A,c)$ denotes the decoder that recreates statistics from instance and the restricted possibility sharing; and $W[\log M(Z|p,c)$ is the greatest probability assessment to plan the in $A$ and situation c to the qualified hidden state $m(p,c)$. During the preparation phase, additional effort that appears in one hot vector serves as identification for the effort. The CVAE has been trained to generate the production research, which also generates a casual output by collection from the haphazard vector $p$ or the trial from a specific amount and depends on that model, besides the independent position in the hidden area drawn from the conventional usual allocation. The CVAE manipulates and decides certain information from the sampling hidden state.

### *G. Advanced Encryption Standard (AES)*

AES is a key encryption technology that protects consumer database such as borrow history, reservation details, and account credentials before it is saved or transmitted across the blockchain network. The primary purpose is to avoid unauthorized access and safeguard sensitive information against potential threats. AES utilizes group iteration with a patch size of 4 × 4 matrix. Each component has 8 bits. To enhance encryption safety, effectiveness, and productivity, research provides the following enhancements to the AES algorithm's foundation. The AES algorithm is a symmetrical key method that has been approved as the standard for encrypting digital data. It is an iterative circular cipher that operates on 128-bit plaintext with three distinct key lengths. The key length regulates the number of encryption and decryption phases, depending on their mathematical strength. The AES algorithm includes four invertible transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The encryption rounds apply each transform except the final phase, which eliminates the MixColumns alteration to render the encryption and decryption schemes symmetric. The ETSO algorithm optimizes the encryption keys in AES for enhanced performance and reduced computational overhead, resulting in more robust security. This strategic use of AES guarantees that only authorized parties can decrypt and access the data, which reinforces the BESLRM system's overall security architecture.

### *H. Efficient Transient Search (ETS)*

The idea of transitivity is inspired by the transient properties of electronic systems that include energy storage components like capacitance and inductors. A beginnings circuit is a power supply that comprises resistance and an individual batteries device, whereas a secondary circuit has a barrier as well as two resource storage elements. Energy storage systems provide a time delay in the change of electrical properties, such as inductor current and capacitor voltage, following the actuation of a valve. These attributes cannot be changed instantly, which is referred to as the circuit's transient response. The transient reaction changes according to the circuit's sequence. Equation (2) describes the computational structure of first-order circuits, while Equation (3) responds:

$$\frac{c}{cs}w(s) + \frac{w(s)}{\tau} = L, \quad (2)$$

$$w(s) = w(\infty) + \big(w(0) - w(\infty)\big)f^{\frac{-s}{s}} \quad (3)$$

During fluctuations, second-order network behavior can be represented by employing the 2nd order differential method, as determined in Equation (4).

$$\frac{c^2}{cs^2}w(s) + 2\alpha\frac{c}{cs}w(s) + \omega_0^2 w(s) = e(s) \quad (4)$$

The response to the listed second-order differential Equation (5) is shown below.

$$w(s) = f^{-\alpha s}(A_1 \cos(2\pi e_c s) + A_2 \sin(2\pi e_c s))\infty) \quad (5)$$

Here $w(s)$ represents the fluctuating voltages across the circuit's capacitors or energy passing through the inductor. τ is the time constant, while α is a dampening coefficient. $\omega_0^2$ and $e_c$ represent the decreased and resonant frequencies, respectively, whereas $A_1$ and $A_2$ are constants. Equation (6) illustrates the modification of search agents in the TS, while Fig. 2 highlights the TS technique for locating the global solution.

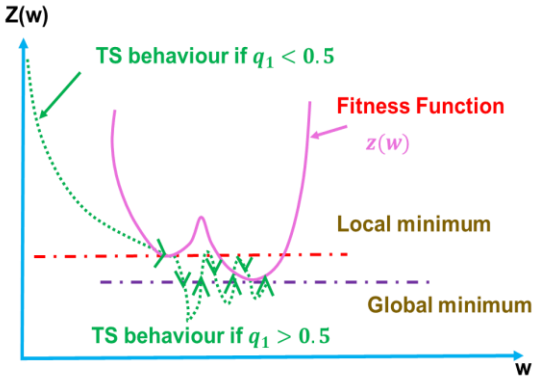


Fig 2. Identifying the TS Strategy

Equations (7-9) depict the computational phases of discovering and extracting the TS.

$$Z_{s+1} = \begin{cases} Z_s^* + (Z_s - D \cdot Z_s^*) f^{-S} q_1 < 0.5 \\ Z_s^* + f^{-S}[\cos(2\pi S) + \sin(2\pi S)]|Z_s - D.Z_s^*|q_{1\geq 0.5} \end{cases} \quad (6)$$

$$S = 2 \times b \times q_2 - b \quad (7)$$

$$D = l \times b \times q_3 + 1 \quad (8)$$

$$b = 2 - 2 \times \left(\frac{s}{s_{max}}\right) \quad (9)$$

$S$, $D$, $q_1$, $q_2$, and $q_3$ are all randomly produced numbers. $Z_s$ Represents the population's current location, while $Z_s^*$ represents its optimal position. The parameters $S$ and $s_{max}$ represent the current iteration number, where as $l$ maintains a constant. The '$S$ ' parameter balances the stages of identification and removal. The value of $'\sigma'$ is defined as $[-2, 2]$. A positive value for '$S$ ' suggests the supremacy of the exploitative process, while a negative value suggests the superiority of the prospecting phase.

The research endeavors to increase the efficacy of the Traditional Search and Exploration Orientation method by modifying search agent updating mechanisms. ETS has concerns such as asymmetry between the prospecting and extraction stages and early convergence. The Rosenbrock Direct Rotation Technique (RDRT), developed to handle the specific characteristics of the banana function, whose lowest point occurs within a secure, curved valley, is utilized to address the challenge. RDRT uses adaptive direction and sizing for the search, beginning with the initial search utilizing the coordinate axes trajectory. At least one unsuccessful search direction is tried before effective moves are accomplished.

Once the process succeeded, it recalibrates its orthonormal foundation to include the aggregate impact of all successful motions in all paths, as well as the single action that failed to culminate in the desired result. In addition, it resets the step sizes to their original values. The Gram-Schmidt orthonormalization procedure, also known as Palmer's approach, is used to alter the orthonormal basis, as shown in Equation (10).

$$w^{l+1} - w^{l+} = \sum_{j=1}^{m} \lambda_j \cdot c_j, \quad (10)$$

Equation (11) illustrates the updated approach directions, with $\lambda_j$ denoting the aggregate count of favorable variables and $w^{l+1} - w^{l+}$indicating the most beneficial direction coming from the recently ended phase. As a consequence, this direction is integrated into the modified query path.

$$Oj = \begin{cases} c_j, \lambda_j = 0 \\ \sum_{i=j}^{m} \lambda_i \cdot c_i, \lambda_j \neq 0 \end{cases} \quad (11)$$

Equation (12) is subsequently modified with the obtained results, which have been improved utilizing the Gram-Schmidt reduction approach. After uniformity, the updated query parameters are as follows in Equation (13):

$$rj = \begin{cases} O_j, j = 1 \\ O_j - \sum_{i=1}^{j-1} \frac{r_i^s \cdot oj}{r_i^s \cdot r_i}, j \geq 2 \end{cases} \quad (12)$$

$$c_j = \frac{r_j}{\|r_j\|}, j = 1,2, \ldots, m \quad (13)$$

The exploration is repeated cyclically across the brand-new diagonal paths, and the cycle continues until certain terminating requirements are achieved.

ETS-CVAE improves security by evaluating encrypted data only at approved endpoints while maintaining post-decryption privacy. Algorithm 1 represents the ETS-CVAE method.

***Algorithm 1: Efficient Transient Search-driven Conditional Vibrational Auto encoder (ETS-CVAE)***

```
# CVAE Encoder
def encoder(input_data, condition):
  Z = feed_forward_network(input_data, condition)
  return Z.split()

# Reparameterization
def reparameterize(mean, log_var):
  return mean + exp(0.5 * log_var)
                * random_normal_noise()

# CVAE Decoder
def decoder(Z, condition):
```

```
  return feed_forward_network(Z, condition)

# Loss Function
def loss_function(original, reconstructed,
mean, log_var):
  return compute_mse(original, reconstructed)
                + −0.5 * sum(1 + log_var − mean
                ** 2 − exp(log_var))

# ETS Initialization
def initialize_agents(pop_size, space):
  return [random_initialization(space)
for _ in range(pop_size)]


# ETS Agent Update
def update_agent(agent, best, params):
  S = 2 * params['b'] * random_number()
                − params['b']
  D = params['l'] * params['b']
                * random_number() + 1
  return best + exp(−S) * (cos(2 * pi * S)
                + sin(2 * pi * S)) * abs(agent
                − best)

# Main Training Loop
def train_CVAE_with_ETS(data, conditions,
pop_size, space, epochs, max_iter):
  agents = initialize_agents(pop_size, space)
  best_agent = agents[0]
  best_fitness = fitness_function(best_agent)

  for epoch in range(epochs):
    total_loss = 0
    for d, cond in zip(data, conditions):
      mean, log_var = encoder(d, cond)
      Z = reparameterize(mean, log_var)
      rec_data = decoder(Z, cond)
      total_loss +
= loss_function(d, rec_data, mean, log_var)

    for agent in agents:
      new_agent
= update_agent(agent, best_agent, parameters)
      new_fitness = fitness_function(new_agent)
      if new_fitness < best_fitness:
        best_fitness, best_agent
              = new_fitness, new_agent

    print(f"Epoch {epoch
+ 1}/{epochs}, Loss: {total_loss}, Best Fitness:
{best_fitness}")


  return encoder, decoder, best_agent

# Prediction
def predict_with_CVAE_and_ETS(data, cond,
encoder, decoder, best_agent):
  mean, log_var = encoder(data, cond)
  Z = reparameterize(mean, log_var)
  rec_data = decoder(Z, cond)
  return rec_data, optimize_with_best_agent
(rec_data, best_agent)
```

The algorithm estimates demand trends based on user interactions, allowing libraries to better manage their book collection, eliminate inefficient acquisitions, and maximize resource use. The ETSO-CVAE speeds up model training and improves convergence, lowering computing costs and making the model more suitable for real-time library operations. ETSO-CVAE predicts user preferences for books and digital resources. The system's optimization process enhances its capacity to detect irregular borrowing patterns, which helps with fraud protection, account abuse detection, and system misuse notifications.

## IV. RESULTS

This research aims to develop a BESLRM system using DL for enhancing security and efficiency, by comparing its performance and security advantages with conventional LRM systems. The framework developed using Python 3.9 and libraries, such as TensorFlow and Scikit-learn, on an experimental system consisting of an Intel Core i7, 16 GB RAM, and Windows 10. This result evaluates the proposed BESLRM system's performance in terms of security, efficiency, and forecast accuracy. It emphasizes critical metrics like encryption/decryption times, security levels, and the ETS-CVAE model's performance.

### *A. Security Evaluation and Analysis*

The security assessment examines encryption and decryption times, decision methods, and access protocols to ensure efficient data security and minimize computing cost in real-time processing to achieve confidence, authenticity, and the integrity in blockchain management systems.

### *B. Encryption Time*

Encryption time plays a crucial role in the responsiveness of a blockchain-based library records system. The intention is to identify efficient encryption methods that secure sensitive data while maintaining system throughput. The purpose is to balance robust security with minimal computational overhead, enabling real-time processing of user interactions with the library system. Table I and Fig. 3 represent the significance of encryption time.

TABLE I NUMERICAL FINDINGS OF ENCRYPTION TIME

| Epochs | Encryption Time (Sec) |
|---|---|
| 10 | 28 |
| 20 | 24 |
| 30 | 19 |
| 40 | 15 |
| 50 | 13 |

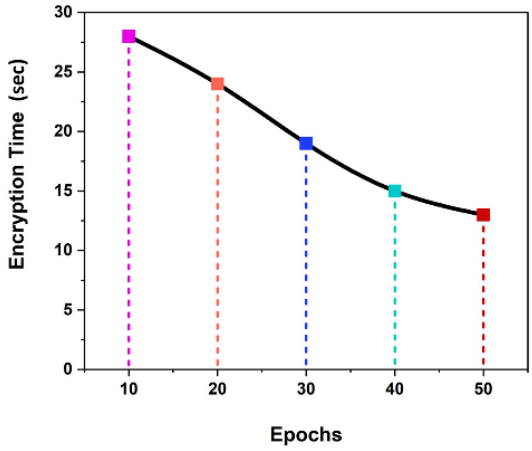


Fig.3 Findings of Encryption Time

Table I shows that the number of epochs evolves from 10 to 50; the encryption time rapidly lowers from 28 to 13 seconds. This pattern suggests that with regular instruction, the model becomes more efficient at handling encryption positions.

### C. *Decryption Time*

Decryption time directly affects how rapid users or systems access stored information. In a decentralized circumstance, it is dynamic to ensure low-latency decryption while protecting data security. Fig. 4 and Table II focus on evaluating decryption performance and determining their suitability in library systems that require both speed and reliability.

TABLE II NUMERICAL FINDINGS OF DECRYPTION TIME

| Epochs | Decryption Time (Sec) |
|---|---|
| 10 | 30 |
| 20 | 27 |
| 30 | 23 |
| 40 | 17 |
| 50 | 15 |

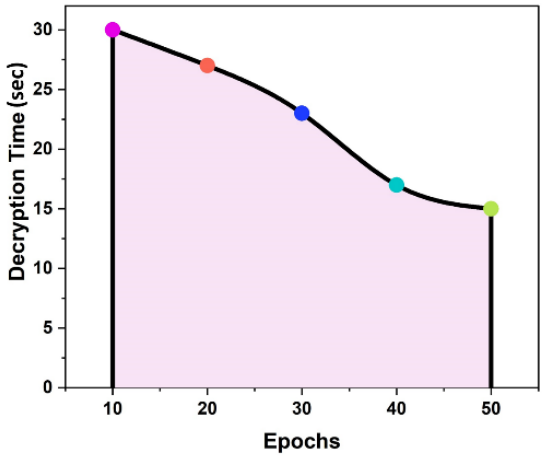


Fig.4 Findings of Decryption Time

Table II determines that the number of epochs increases from 10 to 50; the decryption time decreases from 30 to 15 seconds. This indicates that more training improves the model's efficiency, leading to faster decryption performance.

### D. *Security Level*

Security level represents how well the system safeguards against unauthorized access, data manipulation, and potential breaches. This sector proposes to evaluate the strength of implemented encryption algorithms, consensus mechanisms, and access protocols (Fig. 5 and Table III).

TABLE III NUMERICAL FINDINGS OF SECURITY LEVEL

| Epochs | Security level (%) |
|---|---|
| 20 | 60 |
| 40 | 73 |
| 60 | 86 |
| 80 | 90 |
| 100 | 95 |

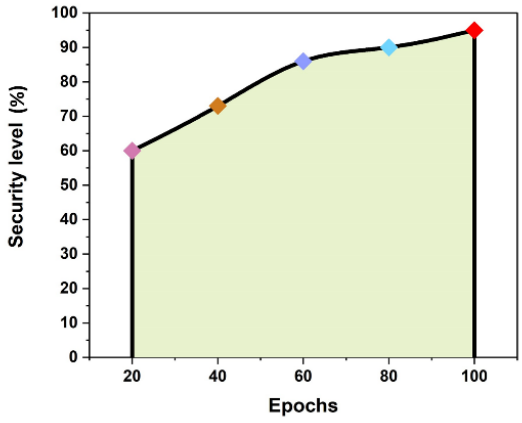


Fig.5 Performance of Security Level

Table III illustrates that as training epochs progress, the security level of the BESLRM system continuously increases. Initially at 60% after 20 epochs, it increases to 73% at 40, 86% at 60, 90% at 80, and 95% at 100 epochs. It demonstrates that more training improves the system's data security effectiveness. The goal is to ensure a high degree of trust, transparency, and immutability in the handling of library records within the blockchain infrastructure.

### E. *Performance Metrics*

The proposed ETS-CVAE approach performed effectively in the circumstances of the BESLRM system, generating the following outcomes, such as accuracy, recall, precision, F1-score, and kappa to evaluate the efficiency. Table IV determines the numerical outcome of the ETS-CVAE proposed approach and Fig. 6 illustrates the graphical visual evaluation of the proposed technique.

*1. Accuracy*

Accuracy is a frequently used statistic for evaluating the efficacy of classification models, representing the proportion of perfect forecasts among all predictions (Equation 14).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (14)$$

The proposed ETS-CVAE model demonstrated a high level of correct predictions (98%), indicating its strong capability to precisely estimate user preferences and identify unusual usage designs in the library system.

*2. Precision*

Precision is a statistic that assesses the quantity of accurate positive forecasts provided by the model. It is computed as follows in Equation (15).

$$Precision = \frac{TP}{TP+FP} \quad (15)$$

The proposed ETS-CVAE approach achieves (94%) and the model's effectiveness in minimizing false positives safeguards that the forecast actions, such as book reservations and check-outs, are mostly correct and relevant to user behavior.

*3. Recall*

Recall, referred to as sensitivity, is a statistic that assesses the fraction of actual positive predictions among all positive instances in the set of observations. The computation occurs as follows in Equation (16):

$$Recall = \frac{TP}{TP+FN} \quad (16)$$

The high recall score (96.50%) specifies that the model successfully identifies a large quantity of actual user behavior patterns, minimizing false negatives. This is critical for detecting uncharacteristic actions.

*4. F1-Score*

The F1 score incorporates the accuracy and recall to provide a reasonable assessment of the model's effectiveness. Equation (17) calculates the harmonic mean of accurateness and recollection.

$$F1 - Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \quad (17)$$

The stability between precision and recall is characterized by the F1-score, and with a value of 95.89%, the model performs exceptionally well in preserving a balance between recognizing exact user actions and minimizing false predictions.

*5. Kappa Score*

The Kappa statistic is employed to assess the amount of agreement to allocate components to separate subcategories. The Kappa score (93%) designates a superior level of arrangement between the model's predictions and the actual consequences, suggesting strong consistency in its forecasting ability. The ETS-CVAE technique, when integrated into the BESLRM system, offers improved security, transparency, resource supervision, and user interaction forecasting, making it a more progressive method than traditional methods.

TABLE IV NUMERICAL OUTCOME OF THE PROPOSED APPROACH

| Metrics | Proposed Outcomes (%) |
|---|---|
| Accuracy | 98 |
| Precision | 94 |
| Recall | 96.50 |
| F1-Score | 95.89 |
| Kappa | 93 |

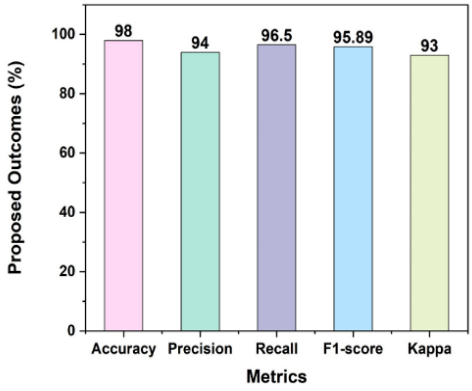


Fig. 6 Visual Assessments of Proposed Approach

*F. Accuracy Loss*

The accuracy loss demonstrates that a modest percentage of the ETS-CVAE models, as represented in Fig. 7, and the findings were inaccurate when predicting user actions in the BESLRM system. The low error rate demonstrates the model's ability to produce reliable and intelligent decisions. It demonstrates that the arrangement handles an enormous quantity of data with the lowest inaccuracy. Overall, the ETS-CVAE technique produces solid and probable outcomes.

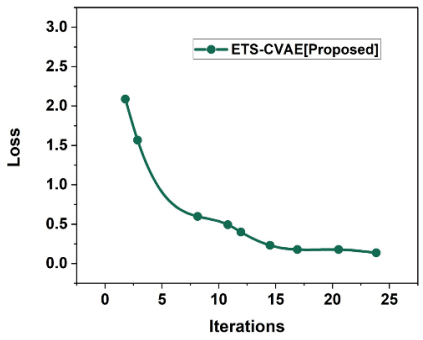


Fig. 7 Graphical Outcomes of Accuracy Loss

The ETS-CVAE model exhibits a loss decrease from 2.0 to 0.4 within 5 iterations, progressively dropping to 0.1 by iteration 25, showing efficient and reliable resolution.

### G. *Area under the Curve - Receiver Operating Characteristic (AUC-ROC)*

The *AUC-ROC Curve* is a metric that measures an identification approach efficiency to distinguish between positive and negative categories at various threshold values. The ROC curve is a valued tool for determining the prospect of a binary effect. False Positive Rate (FPR) (x-axis) versus the True Positive Rate (TPR) (y-axis) for an assortment of potential threshold levels ranging from 0.0 to 1.0. TPR is the amount of a model's ability to reliably forecast beneficial occurrences when they appear. It is calculated using the total number of FPR and an intense assessment of true positives. AUC is an appreciated quantity for assessing the curves of various approaches and assessing their skill. The framework of the curves establishes critical information about the situation, such as the estimated false positive and negative rates. Fig. 8 shows the ROC curve, representing the equilibrium of TPR and FPR at different thresholds.

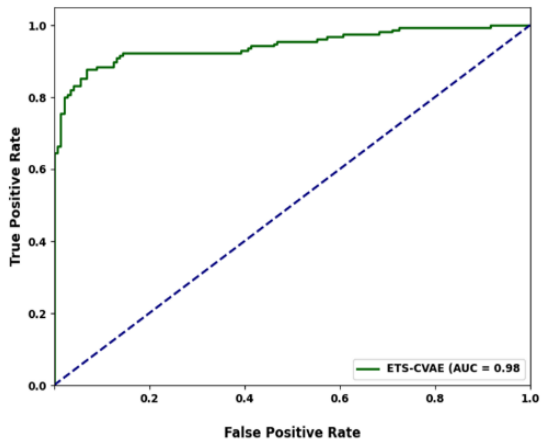


Fig. 8 Graphical Outcomes of AUC-ROC

The ROC curve demonstrates that the ETS-CVAE model has a high AUC of 0.98, suggesting substantial effectiveness in predicting. When the FPR is less than 0.2, the TPR maintains more than 0.9, indicating that the prediction is accurate.

## V. Discussion

In the research, the BESLRM system manages ELRs with blockchain technology and DL, ensuring secure preservation, accessibility, and transparency. It employs AES encryption and ETSO key generation to secure valuable information while maximizing encryption performance with limited operational effort. The adoption of blockchain technology in Nigerian libraries faces challenges, such as technophobia, lack of information, poor technical infrastructure, inconsistent power supply, and inadequate internet access, despite its promising applications (Akintunde &Amuda, (2024). Research identified infrastructure expenses, security issues, and insufficient awareness among librarians as key barriers (Tella et al., 2022). The difficulties include high maintenance costs, and sustainability concerns as barriers to utilizing blockchain for archives and libraries (Manda, 2024). While blockchain improves identity management in telecom services, regulatory compliance and integration complexity remained unsolved issues (Manakhari & Jadhav, 2024). Research highlighted that classic federated learning problems with non-IID data distribution, necessitating advanced blockchain-based hierarchical frameworks to address privacy and performance concerns (Verma, 2025). The proposed BESLRM system improves security, improves resource management using the ETS-CVAE paradigm, and provides transparency through decentralized transaction records, promoting certainty and dependability in the activities of libraries. Its low error rate and great consistency in model forecasts demonstrate its ability to manage huge database while minimizing errors. The AUC-ROC curve investigation demonstrates its accuracy in discriminating between true and false positive user interactions.

## VI. Conclusion

The research studied how the BESLRM system efficiently addresses the challenges of data security, access control, and resource management in the ELRs. By integrating a block chain technology, the structure guarantees secure, decentralized data storage and advances transparency in library operations. The application of AES for encryption, along with the ETSO for key generation, guarantees optimal encryption performance. Furthermore, the ETS-CVAE model accurately forecasts user preferences and detects unusual usage patterns, significantly improving library resource administration. The classification established impressive performance metrics, including a precision of 94%, recall of 96.50%, accuracy of 98%, F1-score of 95.89%, and a Kappa score of 93%.

### A. *Limitations and Future Scope of the Research*

The BESLRM system has scalability and computational overhead complications, which require specific apparatus and training. Future research should focus on cumulative scalability, optimizing blockchain performance, and integrating decentralized storage options.

## References

[1] Ajani, Y. A., Tella, A., Salawu, K. Y., & Abdullahi, F. (2022). Perspectives of librarians on awareness and readiness of academic libraries to integrate artificial intelligence for library operations and services in Nigeria. *Internet Reference Services Quarterly*, *26*(4), 213-230. https://doi.org/10.1080/10875301.2022.2086196

[2] Akintunde, M. O., & Amuda, H. O. (2024). Predictors of adoption of blockchain technology by academic libraries in Nigeria. *Library Hi Tech*. https://doi.org/10.1108/LHT-06-2023-0247

[3] Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences*, *11*(12), 5585. https://doi.org/10.3390/app11125585

[4] Alhassan, S., Abdul-Salaam, G., Micheal, A., Missah, Y. M., Ganaa, E. D., & Shirazu, A. S. (2024). CFS-AE: Correlation-based Feature Selection and Autoencoder for Improved Intrusion Detection System Performance. *Journal of Internet Services and*

*Information Security*, *14*(1), 104-120. https://doi.org/10.58346/JISIS.2024.I1.007

[5] Almolhis, N. A. (2024). A Bayesian-Network Approach for Assessing Security and Process Safety in the Petroleum Industry. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(4), 335-347. https://doi.org/10.58346/JOWUA.2024.I4.022

[6] Ashtagi, R., Rajput, V., Mohite, S., Musale, V., Jaybhaye, S. M., & Bidwe, R. V. (2024). Utilizing Blockchain for Enhanced Security and Transparency in Library Transactions. *Library of Progress-Library Science, Information Technology & Computer*, *44*(1), 123-141.

[7] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy, 2*(2), 29-40.

[8] Farhang, A., & Rashidi, H. (2015). A modify fingerprint watermarking to improve Security in Wireless Networks. *International Academic Journal of Science and Engineering, 2*(2), 95–108.

[9] Fasola, O. S., Oyadeyi, A. E., &Iyoro, A. O. (2024). Awareness, Acceptance and Readiness to Use Blockchain Technology for Library Services in Academic Libraries in Nigeria. *Communicate: Journal of Library and Information Science, 26*(1), 270-288.

[10] Khan, A. U., Jan, S. U., Khan, M. N., Aziz, F., Sohu, J. M., Ali, J., Khan, M. & Chohan, S. R. (2024). Based on the S–O–R theory adoption intention of blockchain technology in libraries: a two-stage analysis SEM–PLS and ANN. *Library Hi Tech.* https://doi.org/10.1108/LHT-03-2024-0128

[11] Kim, J. (2024). Leading teachers' perspective on teacher-AI collaboration in education. *Education and Information Technologies, 29*(7), 8693-8724. https://doi.org/10.1007/s10639-023-12109-5

[12] Manakhari, S. S., & Jadhav, A. P. (2024, July). Enhancing data security with decentralized cloud storage: an IPFS approach. *In World Congress in Computer Science, Computer Engineering & Applied Computing* (pp. 27-39). Cham: Springer Nature Switzerland.https://doi.org/10.1007/978-3-031-85884-0_3

[13] Manda, J. K. (2024). Blockchain-based Identity Management in Telecom: Implementing Blockchain for Secure and Decentralized Identity Management Solutions in. Available at SSRN 5136783.

[14] Meng, H., Ding, J., Wang, H., Zhang, Z., Yao, X., & Ning, H. (2025). Blockchain Enabled Metaverse: Development and Applications. *Tsinghua Science and Technology*, *30*(4), 1552-1582. https://doi.org/10.26599/TST.2024.9010054

[15] Okunlaya, R. O., Syed Abdullah, N., & Alias, R. A. (2022). Artificial intelligence (AI) library services innovative conceptual framework for the digital transformation of university education. *Library Hi Tech, 40*(6), 1869-1892. https://doi.org/10.1108/LHT-07-2021-0242

[16] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research*, *10*(2), 01–09. https://doi.org/10.9756/IAJIR/V10I2/IAJIR1004

[17] Puzier, L. M., & Nous, R. A. (2022). System Statuses in Academic Libraries: Increasing Transparency and Improving the User Experience. *Journal of Library & Information Services in Distance Learning*, *16*(3-4), 182-202. https://doi.org/10.1080/1533290X.2022.2131694

[18] Tella, A., Amuda, H. O., & Ajani, Y. A. (2022). Relevance of blockchain technology and the management of libraries and archives in the 4IR. *Digital Library Perspectives, 38*(4), 460-475. http://dx.doi.org/10.1108/DLP-08-2021-0065

[19] Verma, R. (2025). The future of academic libraries: Blockchain for secure and transparent information management. *In Driving Socio-Economic Growth With AI and Blockchain* (pp. 401-432). *IGI Global Scientific Publishing.* https://doi.org/10.4018/979-8-3693-8664-4.ch017

[20] Zhang, F., Zhang, Y., Ji, S., & Han, Z. (2024). Secure and decentralized federated learning framework with non-IID data based on blockchain. *Heliyon*, *10*(5), e27176. https://doi.org/10.1016/j.heliyon.2024.e27176