INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Blockchain Powered Spatio-Temporal Deep Learning for Decentralized Digital Identity Management

C Vignesh[1]*, M Chidambaram[2]

1 Research Scholar, Department of Computer Science, Rajah Serfoji Government College (Autonomous; Affiliated to Bharathidasan University, Tiruchirappalli - 620 024), Thanjavur-613005, Tamil Nadu, India
2 Research Supervisor cum Associate Professor, Department of Computer Science, Rajah Serfoji Government College (Autonomous; Affiliated to Bharathidasan University, Tiruchirappalli - 620 024), Thanjavur-613005, Tamil Nadu, India

OPEN ACCESS

Received: 05/10/2026
Accepted: 02/11/2026
Published: 16/11/2026

Citation: Vignesh C, Chidambaram M (2026) Blockchain Powered Spatio-Temporal Deep Learning for Decentralized Digital Identity Management. Indian Journal of Science and Technology 19(41): 2786-2803. https://doi.org/10.17485/IJST/v19i41.1340

* **Corresponding author**.

cs.vignesh72@gmail.com

Funding: None

Competing Interests: None

Copyright: © 2026 Vignesh & Chidambaram. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The digital landscape increasingly depends on data exchange, highlighting the significance of Decentralized Digital Identity Management (DDIM) for secure and seamless digital interactions. **Method:** The study proposes a blockchain-based DDIM method called Spatio-Temporal Attention-based Deep Learning (STA-DL). It uses registration, Spatial-Temporal Attention-based Deep Long Short-Term Memory for fraud feature extraction from driver's license details, and X.509 blockchain with Proof-of-Work (PoW) for privacy-preserving fraud detection and two-step authentication. A prototype was implemented to evaluate its performance using 6,000 samples. **Findings:** The experimental results demonstrate that the proposed STA-DL achieves an accuracy of 0.93, precision of 0.90, and recall of 0.95 for fraud detection. It also achieves a transaction throughput of 5085 TPS and a latency of 11.35 seconds on 6,000 samples. The proposed architecture integrates Spatio-temporal deep learning with blockchain-based identity management to improve fraud pattern detection and secure decentralized digital identity management. **Novelty:** Compared with existing attention-based fraud detection methods, STA-DL combines spatial and temporal attention within a deep LSTM architecture (STA-DLSTM) specifically designed for digital identity document analysis. This design aims to identify discriminative identity document features and capture long-range dependencies that are useful for distinguishing genuine and fraudulent identity documents. Compared with conventional blockchain-based identity management methods, which focus on decentralized record management and transaction verification, STA-DL incorporates attention-based fraud feature extraction and document-level validation into the identity management workflow. An identity validation mechanism integrating X.509 digital certificates with blockchain transaction verification through Proof-of-Work is incorporated to support certificate-based identity verification and decentralized transaction validation.

Keywords: Decentralized Digital Identity Management; Blockchain; Spatio-Temporal Attention; Deep Learning; Proof-of-Work

1 Introduction

The swift evolution of the Internet over recent years has resulted in numerous changes causing the emergence of a new paradigm, called, Decentralized Digital Identity System via Web 3.0. Web 3.0 denotes the next generation of internet classified by a decentralized architecture that uses blockchain technology to improve security and interoperability. Existing DDIS solutions struggle with limited scalability issues, constraining their appropriateness in large-scale ecosystems.

A Multi-layer blockchain-based Decentralized Digital Identity (MDID) was proposed in [1] via a four-layer architecture that boosts both interoperability and scalability across different DID systems. To ensure security, Redundant Byzantine Fault Tolerance (RBFT) consensus protocol was used along with a threshold signature algorithm to provide robust decentralization. Moreover, the application of Sharded Merkle Patricia Tree (SMPT) further optimizes efficient storage and retrieval therefore minimizing time and E2E latency. In spite of minimal time and latency involved, however the precision involved in MDID was not emphasized.

A zero-trust for DDIM was proposed in [2] using machine learning based detection methods to combat against cyber-attacks. Owing to the reason that trust is not entirely a technical compliance issue, the method also used fuzzy logic to ensure customization, therefore resulting in adaptability across different environments without compromising trust levels. With this design resulted in the improvement of latency and minimization of computation, communication cost. Though both communication, computation cost along with latency was improved, however the transaction throughput involved in DDIM was not focused.

A blockchain-driven identity management called Self-Sovereign Digital Identity (SSDI) was proposed in [3] with the objective of enhancing traceability with application domain of forest supply chains. Also, with introduction of digital identity verification and decentralized records resulted in improved transparency. Data streamline handling was also provided therefore improving transactions rates and latency. Finally, by incorporating monitoring and digital tools promoted sustainability. In spite of improved transaction rates along with latency, however, the precision and accuracy factors involved in SSDI were not concentrated. A lightweight deep learning model was proposed in [4] for digital identification reducing model complexity.

Over the recent years, the swift expansion of digital services along with the resources on Industrial Internet has inflicted higher demands on privacy of identity management. Specifically with the evolution of the digital economy, sensible users are encouraged to maintain control over their digital identity credentials. A robust UAV identity management technique was proposed in [5] therefore ensuring attack resistance mechanism accurately.

A method to improve cyber physical systems based on ontology was presented in [6] to ensure verifiable query of identity and associated industrial data. However, the single points of failure in turn cause excessive disclosure. To address on this aspect, a privacy-enhanced DDIMs was proposed in [7] using verifiable credentials, therefore, ensuring hierarchical identity authentication.

The digital outlook heavily depends on data exchange, highlighting the significance of DDIM systems. Nevertheless, current methods pose susceptibilities resulting in the insistence of more secure and decentralized DDIM systems. A biometric identity management system was presented in [8] with the aid of proof of concept making it tamper-proof and ensuring security. Yet another comprehensive security protocol using blockchain-based decentralized architecture was proposed in [9] therefore providing trust and security. However, the accuracy factor involved in blockchain-based decentralized architecture was not focused. To address this aspect, a machine learning algorithm was designed in [10] ensured both accuracy and scalability. A comprehensive survey to digital identity management ensuring security and trustworthiness was investigated in [11].

A holistic literature review on blockchain-based identity management system was presented in [12]. Traditional DDIM system lack transparency and are highly susceptible to single-point failure. A blockchain-aware decentralized identity management along with access control model was proposed in [13] to combat against the transparency issue. Yet another digital twin management system employing optimization algorithm along with blockchain framework was presented in [14] with improved convergence rate and minimal response time. A practical method to secure DDIM system employing privacy preserving identity attribute management scheme was proposed in [15] with improved transaction per second results.

1.1 Research gap

Existing decentralized digital identity systems mainly focus on the blockchain side, such as decentralized record storage, access control, scalability and transaction verification. These systems keep identity records safe once they are stored, but they do not check whether the identity document itself is genuine, so a forged document can still be registered and accepted. On the other hand, deep learning (DL) methods analyze identity document images to detect forgery, but they usually do not store their results in a form that is tamper-evident and verifiable by others. Few studies bring these two sides together in a single framework, and even fewer evaluate fraud detection quality (accuracy, precision, recall) along with blockchain performance (throughput,

latency) on a common dataset. This gap motivates the proposed STA-DL framework, which joins attention-based document analysis with certificate-based verification and Proof-of-Work-based ledger integrity.

1.2 Contributions of the work

- To address the above said issues, namely, improving Precision and Recall in fraud pattern detection on the IDNet dataset, STA-DL is designed. The novelty and contributions of the STA-DL are listed as given below.
- Proposed STA-DL framework is designed by integrating identity registration, Optimal Global Threshold-based image preprocessing, feature extraction, and blockchain-assisted identity validation for digital identity fraud detection.
- The proposed framework is evaluated using fraud detection accuracy, precision, recall, transaction throughput, and latency and compared with baseline methods on the IDNet dataset.

1.3 Related Works

The advent of blockchain technology has made an in surgence in the area of cyber security. Given that on the internet, almost every interaction indulges certain digital identity, hence the ways required to safeguard the digital identity over the internet become stronger. A decentralized digital identity system for web 3.0 applications was proposed in [16] that in turn ensured low end to end latency. Yet another method to ensure smart learning process employing blockchain based deep learning framework was designed in [17] therefore achieving a high degree of accuracy with minimal loss. A work focusing on managing on-chain and off-chain decentralized digital identities was proposed in [18] to ensure accurate validation. A holistic review on blockchain-based identity management was presented in [19] with primary studies published between 2009 and 2020.

With the digital era, digital identity is becoming one of the primary components with more processes and interactions being occurring in the digital sphere. Hence, prevailing identity management mechanisms has to define how these associations will look in the future. However, different communities frequently view management with their own solutions in spite of their similarities. To ensure both security and scalability a blockchain approach employing hyperledger fabric was designed in [20] therefore reducing fraud and errors. A privacy-protection scheme employing zero knowledge proof and Shamir secret sharing was proposed in [21] to ensure data integrity. A detailed analytical approach focusing on transaction throughput and latency was presented in [22] by digitally securing supply chain management practices.

A multi-factor authentication mechanism was designed in [23] ensuring improvement in accuracy and precision. A comprehensive requirement for enterprise software was detailed in [24]. A collaborative framework incorporating machine learning, deep learning and federated learning was proposed in [25] that with the use of decentralized identifier in turn minimized dedicated time for completing credential operations.

In spite of the notable progress made by the aforementioned all-in-one methods, most of them depend on focusing precision or transaction latency separately. As a consequence, they are susceptibletoperformancedegradationinfraudpatterndetectioninvolvingimagesandmetadata. In addition, the lack of an explicit feature extraction technique both in the image and metadata limits their adaptability to novel types of identity documents. To address these challenges, blockchain-based decentralized digital identity method called, method Spatio-Temporal Attention-based Deep Learning (STA-DL) with minimal latency and maximum transaction throughput, accuracy is designed.

2 Methodology

2.1 Dataset Description

The IDNet: A Novel Dataset for Identity Document Analysis and Fraud Detection extracted from https://zenodo.org/records/13854938 is used toper form DDIM via blockchain framework with the intent of detecting fraudulent patterns. The dataset includes 597,900 images of synthetically produced identity documents. The identity document includes driver licenses from 10 U.S. States and passport/ID cards covering 10 European countries. Also to ensure privacy-preservation fraud detection a new benchmark dataset was employed for easily accessing and validation.

2.2 Decentralized Digital Identity System using Spatio-Temporal Attention-based Deep Learning

The DDIM system is a collection of policies and technologies that coordinate with the intent of ensuring that the pertinent users within an organization have access to technology resources such. It protects against illegal access to systems and resources by generating alert when unauthorized user try to access information. The research extremely focuses on designing the fraud

detection mechanism by applying the Decentralized Digital Identity System using Spatio-Temporal Attention-based Deep Learning (STA-DL) method. Figure 1 shows the flow diagram of the STA-DL method.

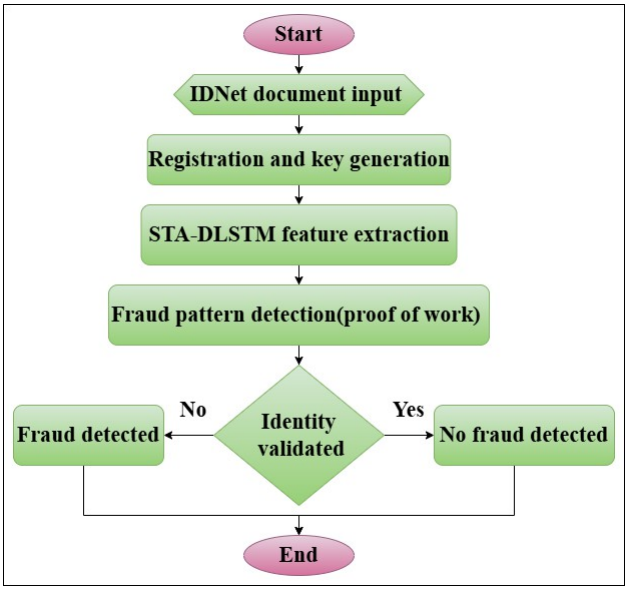

Fig 1. Flow diagram of the STA-DL method

The proposed system works in three phases. During registration, the user's identity document details (name, age, birthday, gender) are signed with RSA keys and stored in a block of the blockchain, and the user receives login credentials and a private key and address. The STA-DLSTM model is then applied to the document image. The IDNet dataset is used for training. The image is preprocessed with Optimal Global Threshold, features are extracted with spatial and positional attention, and the Deep LSTM classifies the document as genuine or fraudulent. It handles five fraud classes (in paint and rewrite, crop and move, face morphing, portrait substitution, text field replacement) and mixed fraud. This model is the only component that performs fraud detection. Based on the analysis report, an X.509 certificate is issued. It binds the user's public key, document information (licence number) and the digital signature, and it provides authenticity and non-repudiation. It does not detect fraud.

The signed certificate is then submitted as a transaction, and Proof-of-Work is used as the consensus mechanism to validate and append it to the blockchain. PoW does not classify documents and does not affect detection accuracy. It makes modification of stored records computationally infeasible, thereby ensuring integrity. During verification, the blockchain server first checks the licence number and then compares the signed document sign (D) with the record stored on the blockchain. Table 1 presents the role of the components in the proposed STA-DL method.

Table 1. Role of the components in the proposed STA-DL method

Component	Question answered	Layer	Output
STA-DLSTM	Is the document genuine or fraudulent?	Detection (off-chain)	Class label and analysis report
X.509 + RSA signature	Who signed the report and is it unaltered?	Authenticity and identity	Signed certificate
Proof-of-Work	Is the record validly and immutably stored?	Consensus and integrity	Mined block in the chain

The detailed process of DDIM for fraud detection via identity document analysis is provided in the following sections.

2.2.1. Registration Phase

The decentralized digital identity system (DDIS) for fraud detection using identity documents starts with the user registration. To register the user's document (i.e.the driver's license or passports or identity cards), certain details are fetched from each user document. The number of documents in the DDIS is represented as given below.

$$D = \{D1, D2, \ldots, Dl, \ldots, DN\} \tag{1}$$

From the above **equation (1)**, 'D' denotes the documents with total number of documents for fraud detection being 'DN'and'Dl' represents the '$l-th$' document. Each document registers the required metadata feature such as name, age, birthday, gender and so on, that are represented as given below.

$$Da(Dl) = \{F1, F2, \ldots., FM\} Dl, M = 14 \tag{2}$$

From the above **equation (2)**, 'F_1', 'F_2', represent the name and the age of the user document respectively, 'F_3' indicates the birthday and 'F_4' denotes the gender of the user respectively. Upon successful completion of the registration, the users with the corresponding document is provided with the identity number, login credentials and separate blockchain private key and address for individual users. The obtained identity document details from the driver are signed and stored in the blockchain. A blockchain '' is mathematically formulated as a linked list of blocks, each consisting of a set of transactions 'T' represented as given below.

$$\mathcal{B} = \{\mathcal{B}1, \mathcal{B}2, \mathcal{B}3, \ldots, \mathcal{B}l, .., \mathcal{B}N\} \tag{3}$$

$$\mathcal{B}i = Ti, evhash, hash(\mathcal{B}i) \tag{4}$$

From the above **equations (3) and (4)** '$prevhash$' denotes the hash of previous block in the blockchain. This mechanism in turn ensures ledger immutability. To encrypt the document details, the asymmetric encryption function is used that not only encrypts document details but also supports digital signatures. The asymmetric encryption function employed in our work ensures high security and provides confidentiality to the users with the corresponding document details.

To generate the key pair, two distinct large random prime numbers 'q' and 'r' are chosen, and the modulus 'n' is computed with the results stored in 'p'.

$$p = n = q * (5) \tag{5}$$

In addition to the above random prime numbers, a public exponent'E' is also selected that lies between '$q-1$' and '$r-1$'. The public exponent is then represented as given below.

$$\varphi\,(p) = (q-1) * (r-1) \tag{6}$$

From the above **equation (6)** '' being the Euler's totient the private component 'h' is represented as given below.

$$h = E^{-1} m(\varphi(p)) \tag{7}$$

From the above **equation (7)** it is inferred that the exponent is the multiplicative inverse of public exponent with Euler's totient. With this the obtained public and private keys are denoted as given below.

$$PubK = (p, E) \tag{8}$$

$$PrivK = (p, h) \tag{9}$$

With the above generation of public and private keys according to **equations (8) and (9)**, the identity documents data are signed and stored for further reference. The user keeps PrivK secret and shares PubK. The identity document data D is signed with the private key as sign (D) = H(D)^h mod n, where H(·) denotes hash function (SHA-256). Anyone holding PubK can verify the signature by checking that sign(D)^E mod n = H(D). The signed document is then stored on the blockchain.

2.2.2. Feature Extraction with Spatial Temporal Attention-based Deep Long Short Term Memory

To perform efficient fraud detection, a Spatial Temporal Attention-based Deep LSTM (STA-DLSTM) is presented in this work. This model is the incorporation of the spatial and positional attention mechanism arranged performed parallel to evaluate the features along with the homogenization of STA-DLSTM to identify the fraudulent documents and hence preserving privacy in an efficient manner. The STA-DLSTM model extracts specific and distinct fraud patterns and long-range relationships from digital identity documents, providing findings into their fraud detection learning trajectory. Although the conventional

LSTM networks employed were susceptible to overfitting as well as complexity in capturing difficult identity documents images and interpretation complexities. In the proposed model such drawbacks are focused by homogenizing the use of Spatial and Temporal attention mechanisms with the STA-DLSTM networks. This in turn aids in optimizing accuracy of fraud detection and dynamically fine tuning the relevance of past learning experiences based on the present learning situation. The proposed fraud detection based on decentralized digital identity system namely, STA-DLSTM is the fusion of spatial and positional attention in the STA-DLSTM. The proposed model for fraud detection feature extraction based on decentralized digital identity system is illustrated in Figure 2.

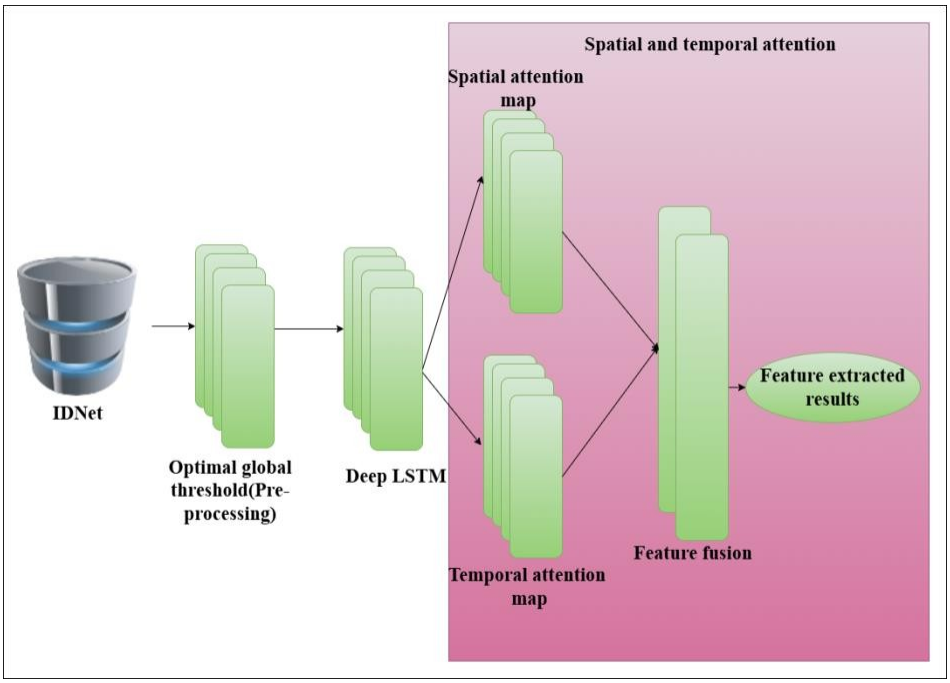

Fig 2. Structure of Spatial Temporal Attention with Deep Long Short Term Memory based Feature extraction

As shown in the above figure, initially, the input digital data document obtained from IDNet dataset is applied to the preprocessing phase, which selects the required data utilized for the fraud detection system. Here initially Optimal Global Threshold based pre-processing is applied to not only standardize raw images but also isolate text from it to maximize accuracy and enhance contrast. Using the Optimal Global Threshold as pre-processing identifies a threshold value that minimizes stacked within class variance. Due to the reason that variance represents the spread of distribution about the mean and reducing this within class variable in turn make the classes compact and ensures efficient differentiation between image and text.

Let us consider we threshold a histogram at a value 'Th'. This histogram threshold then generations two are as, i.e. left and right of'Th' and its variance is represented by 'σ_i^2' and 'σ_j^2' respectively. Then, the stacked within class variance is mathematically defined as given below.

$$\sigma_w^2 = w_i(Th)\sigma_i^2(Th) + w_j(Th)\sigma_j^2(Th) \tag{10}$$

From the above **equation (10)** '(Th)' and '$wj(Th)$' denotes the weights given to each class. Here, weight denotes the total pixels in at thresholds region (i.e. left or right) divided by total image pixels. The preprocessed image is then fed into the Deep LSTM models that by learning, processing and classifying the sequential image data generate the subsequent output. The Deep LSTM architecture follows the decentralized identity management and is activated via tangent as the activation function.

As far as the Deep LSTM model is taken into consideration the cell state here remains the key idea that acts as the blockchain server or carrier to transfer and carry linear interactions between LSTM states. To start with, the LSTM decides the image information that requires the part for fraud detection via the implementation of the sigmoid function. This is mathematically formulated as given below.

$$Fori = Sigmo(WF * [Hi-1, Data(Dl)] + BF) \tag{11}$$

From the above **equation (11)** '$Fori$' denotes the forget gate activated via the '$Sigmoid$' function by using the weight 'WF', hidden state'$Hi-1$' and bias of the forget gate'BF'respectively. Moreover, the generated information is carried on to the next layer that is processed via the sigmoid and tangent function that generate new candidate, and the cell state results as given below.

$$li = Sigmo(Wl * [Hi-1, Data(Dl)] + Bl) \tag{12}$$

$$Ci = Sigmo(WC * [Hi-1, Data(Dl)] + BC) \tag{13}$$

From the above equation 'Ii' represents the input layer activated via the '$Sigmoid$' function by means of weight 'WI' and biases 'BI' respectively. Also, the cell stated is denoted by 'Ci=' possessing weights 'WC' and biases 'BC'. Finally, the vector result is filtered via sigmoid and tangent hyperbolic function to generate the output result as given below.

$$Oi = Sigmo(WO * [Hi-1, Data(Dl)] + BO) \tag{14}$$

$$Hi = Oi \odot tanh(Ci) \tag{15}$$

From the above **equations (14) and (15)** the results of output 'Oi' layer along with the hidden image data information 'Hi' is obtained. The output of deep LSTM is then provided as input to the spatial and temporal attention mechanisms. The purpose of applying the spatial and temporal attention function is to extract the most significant features that extract the most significant features, recreating the spatial and temporal input data information.

On one hand the Spatial Attention function employed in our work spotlights the specific regions of interest (ROI) while suppressing irrelevant background noise. This is performed via Spatial Attention Map (SAM). The SAM is generated with the image features that occur at the inter-spatial relationship in the input. With this highly information portions of the image are extracted. The SAM results are defined as given below.

$$SAM = Sigmo(CF^{7*7}[AvgP(O); MaxP(O)]) \tag{16}$$

From the above **equation (16)** by applying the average pooling '$AvgP$' and max pooling '$MaxP$' the most redundant features are highlighted. Upon successful incorporation of average pooling and maxpooling, the convolution function 'CF' with filter size of'7*7' is applied to produce the SAM results. On the other hand, the Temporal Attention function utilized in our work obtains the most critical portions of the image.

$$TAM = \frac{\exp(A.B)}{\sum \exp(A.B)} \tag{17}$$

$$FE = \sum_{i=1}^{N} (SAM_i, PAM_i) \tag{18}$$

From the above **equations (17) and (18)** by combining the spatial attention map '$SAMi$' and temporal attention map'$PAMi$' results the overall features are extracted for final fraud pattern detection.

2.2.3. Fraud Pattern Detection Model

The fraud pattern detection model mainly focuses on generating identity document analyzed reports. In the proposed method to generate the fraud pattern detection results, identity document analyzed reports, certificates, X509 is used in contrast to the traditional authentication mechanism. The X509 here represents the public key, and the certificate includes the information of the driver's licenses to identify, the public key, and the information of the signature.

The utilization of X509 in the generation of identity document aids in achieving a highly secure decentralized digital identity. With fraudulent activities belonging to five different classes, like, in paint and rewrite fraud, crop and move fraud, face morphing, portrait substitution, text field replacement fraud and mixed fraud pattern, using X509 as public key standard of cryptography a comparison is made whether the samples has been detected with fraud detection of identity documents in any of these two activities (i.e. face morphing and text field replacement). After the model produces the document analysis report, an X.509

certificate is generated for that report. It binds the user's public key, the document details (e.g. licence number) and the issuer's digital signature. It proves who issued or signed the result and that it was not altered. It does not decide whether the document is fraudulent. During verification, the server checks the licence number first, then the signed document sign(D), against the certificate stored on the blockchain.

In the domain of fraud detection via decentralized digital identity system, a two-step authentication process. Initially, the verification process is made with the license number of the driver and then with the signed digital identity documents '$sig(D)$'. The blockchain server validates the signature shared by the user with the signature available on the blockchain of the user. Also, a detailed ground truth comparison between two different classes of activities is performed to generate the final results.

$$si(Di) = sign(D) \tag{19}$$

With the above obtained results as in **equation (19)**, two different fraud patterns are generated with the certificate stored in the blockchain. The users share the digital badge, and the blockchain server verifies it with the issuing authority. The blockchain server straightforwardly approaches the blockchain storage and ensures the certificate is valid or not (i.e. identified with which type of fraud patterns, i.e. face morphing and text field replacement or both). Hence, the incorporation of the X509 certificate generator in addition to the proof of work security improves the overall reliability as well as trustworthiness. PoW is the consensus protocol employed to validate and append the transaction (the signed report plus certificate) to the blockchain. It makes retroactive modification of stored records computationally expensive, because altering a block would require re-mining that block and all following blocks. PoW does not detect fraud and does not verify document content. It protects the stored result from tampering. The pseudo code representation of DDIM using Spatio-Temporal Attention-based Deep Learning is given below.

Algorithm: Spatio-Temporal Attention-based Deep Learning
Input: Dataset'DS',Samples 'S={S1,S2,….,SN}',Features'F={F1,F2,…,FM}'
Output: precise and accurate decentralized digital identity management

1:**Initialize**'M=14','N=6000'
2:**Begin**
3:**For**each Dataset'DS' with Samples'S' and Features'F'
//Registration phase
4:Initialize the document details and according to(1)and(2)
5:**For**each document details create blocks according to (3)and(4)
//Asymmetric encryption
6:Evaluate public exponent function results according to(5) and (6)
7:Evaluate Euler's totient private component function result according to(7) 8: Evaluate public and private keys according to (8) and (9)
9:**Return** public key, private key
10:**Endfor**
//Pre-processing and feature extraction
11:**For** each Dataset'DS'with Samples'S', Features'F', public key, private key
//Optimal Global Threshold based pre-processing
12:Isolateimageportionswith text according to(10)
//Feature extraction
13:Process sequential image data according to (11), (12),(13),(14)and(15) 14: Generate Spatial Attention Map results according to (16)
15:GenerateTemporal Attention results according to(17) 16: **Return** features extracted 'FE'
17:**Endfor**
//Fraud pattern detection
18:**For** each Dataset'DS'with Samples 'S',Features 'F', public key, private key and features extracted 'FE'
19:Generate fraud pattern detection results according to (18)
20: **Return** fraud pattern detected results
21:**End for**
22:**End**

As given in the above algorithm the entire process of DDIM system for fraud pattern detection is split into four stages. First, registration process was carried out to register the user's identity documents. The registered documents were then stored in the blockchain server by creating separate blocks for each transaction. Next, upon successful registration login procedure was carried out. Moreover as the identity documents included both image and metadata, feature extraction was carried out to not only extract the relevant features present in metadata but also in the registered images. This process is carried out by incorporating spatio-temporal attention and long short term memory. By applying this mechanism in turn aids in improving the overall precision and accuracy involved in the DDIM process. Finally with the extracted features (i.e. from images and metadata) are subjected to transaction validation via PoW therefore reducing the overall latency with improved transaction throughput.

2.3 Case Study and Inferences

In this section case analysis of decentralized digital identity management (DDIM) system using STA-DL method via blockchain framework is detailed by performing qualitative analysis. To perform simulation though several 6000 samples are provided in the IDNet dataset, to perform simulation, three samples (one with image being face morphing, text field replacement fraud and mixed fraud pattern) are used. Figure 3 shows the sample digital identity document images used for simulation.



Fig 3. Sample digital identities

As provided in the above samples three digital identities are provided as input. Accordingly for three sample digital identities, registration process is performed. The registration process of corresponding three samples are shown in Figure 4.

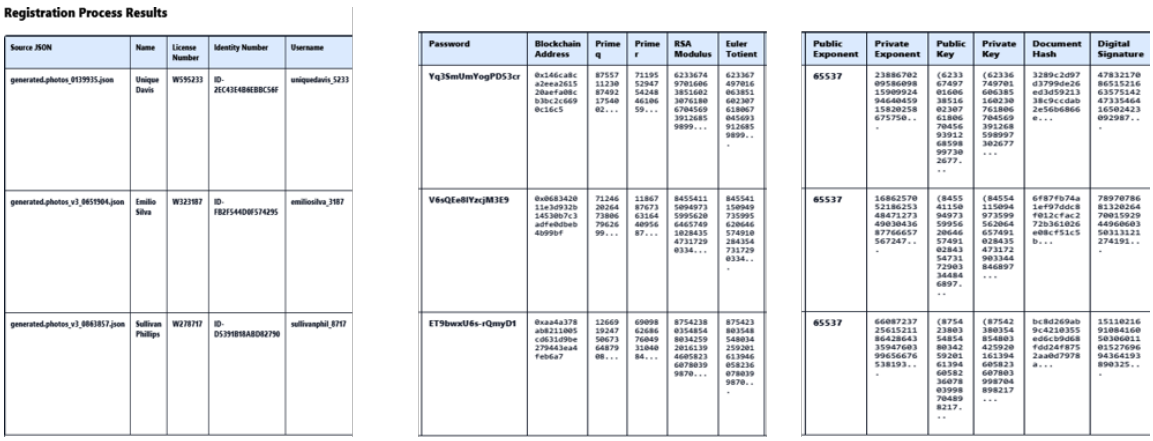

Fig 4. Registration process

As provided in the above results, the registration process is performed by the blockchain in server to perform fraud pattern detection. Followed by which blocks are generated as shown in Figure 6. Upon successful completion of block generation and login completion extraction of features is performed for validation. Figure 5 shows the block chain ledger for corresponding three digital identity documents.

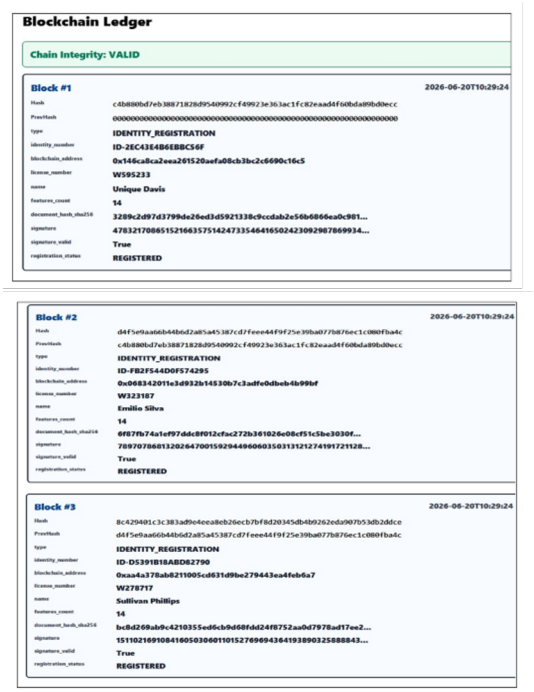

Fig 5. Blockchain ledger generation for three samples

With the above completion of registration process and generation of successful ledger, pre-processing using optimal threshold is performed. This is done to isolate the images from the text. Figure 6 shows the optimal threshold-based pre-processed results.



Fig 6. Isolated text and image based optimal threshold

As provided in the above results by separating the images from the meta data features aids in isolating between the two for further processing. By performing this isolation process in turn not only minimizes latency but also improves the overall transaction throughput. With the pre-processed digital identity samples, relevant image and text features are extracted as shown in Figure 7.

The first figure (of Figure 7) was subjected to image morphing. On the other hand, in case of the second sample, the changes were observed in meta data feature. In case of the third samples, changes were found both by means of image morphing and metadata feature changes. Finally Figure 8 shows the validation results.

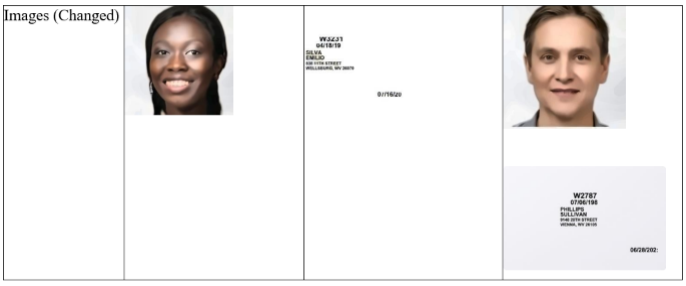

Fig 7. Spatial Attention Map and Temporal Attention Map based feature extraction

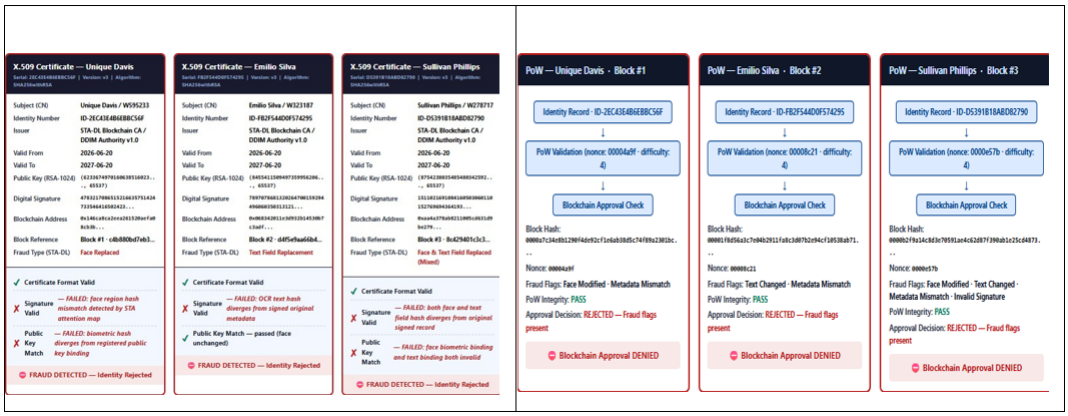

Fig 8. (a) X.509 Certificate Validation (b) Proof of Work of Identity Validated Results

As provided in the Figure 8 results by performing X509 as public key standard of cryptography aids in differentiating between different fraud patterns. By employing this X509 and proof of work as validation aids in providing the fraud pattern results in an accurate and precise manner. The detailed quantitative analysis of fraud pattern detection using DDIM system via blockchain powered framework is provided in the following sub-sections.

3 Experimental setup and Discussion

The proposed STA-DL framework is developed for fraud pattern detection in decentralized digital identity management. The experiments use the IDNet dataset, available from https://zenodo.org/records/13854938. The selected experimental subset consists of 6,000 identity document images. Since the complete IDNet dataset contains a substantially larger collection of synthetic identity documents, the subset selection procedure and the distribution of genuine and fraudulent samples should be specified to establish the scope of the experiments.

The proposed framework is implemented using Python 3.10.11. The reported hardware configuration consists of an Intel Core i7 processor, 8 GB RAM, and 2 TB storage drive. The windows 10 operating environment, processor generation, and GPU availability is utilized. The performance of STA-DL is assessed using fraud detection accuracy, precision, recall, transaction throughput, and latency. The experiments compare the proposed method with the selected baseline approaches, including MDID [1], Zero-trust for DDIM [2], and SSDI [3], using evaluation metrics. Table 2 presents the hyperparameter Configuration of the Proposed STA-DL.

3.1 Implementation details

In this study, we developed the proposed STA-DL for fraud pattern detection.

- The proposed STA-DL is designed with registration, pre-processing, feature extraction and validation.
- We compared our STA-DL method to model to existing MDID[1] , Zero-trust for DDIM[2] and SSDI[3] using IDNet dataset to validating the results.

Table 2. Hyperparameter Configuration of the Proposed STA-DL Framework

S. No.	Hyperparameter	Suggested Value
1	Input Image Size	224×224
2	Spatial Attention Dimension	128
3	Temporal Attention Dimension	128
4	LSTM Hidden Units	128
5	Number of LSTM Layers	2
6	Attention Dropout Rate	0.3
7	Learning Rate	0.001
8	Batch Size	32
9	Number of Epochs	100
10	Optimizer	Adam
11	Weight Decay	0.0001
12	X.509 Certificate Validation	Certificate chain and signature verification
13	Block Size	1 MB
14	Random Seed	42

- Initially, 6000 samples were obtained from dataset.
- Second, Decentralized Digital Identity System, registration along with Optimal Global Threshold based pre-processing is used that isolates images with the text
- Spatial-Temporal Attention-based Deep LSTM combines spatial attention maps and temporal attention maps to identify discriminative document features and capture sequential dependencies among identity-related information. This integrated feature-learning strategy is intended to improve the identification of fraudulent patterns in digital identity documents.
- An integration of blockchain-based identity validation with X.509 digital certificate standards and PoW consensus mechanism. X.509 supports certificate-based identity verification, whereas PoW supports the validation of blockchain transactions. Privacy protection is considered in the identity attribute management process to reduce unnecessary exposure of sensitive identity information.

According to the above implementation patterns, four different evaluation metrics are detailed in the next section.

3.2 Training and Testing and validation procedures

The IDNet dataset subset is divided into training, validation, and testing partitions using 70:10:20 ratio. The training partition is used to optimize the STA-DL model parameters. The validation partition is used to monitor model performance and guide hyperparameter selection. The testing partition is reserved for final performance evaluation and is not used to optimize model parameters or select hyperparameters. The dataset partitioning procedure preserves the relevant class distribution and prevents duplicate or closely related versions of the same underlying identity document from appearing across different partitions. The STA-DL model is trained using the specified optimizer, learning rate, batch size, number of epochs, and regularization settings.

The selected model configuration is evaluated on the held-out testing partition using accuracy, precision, and recall. Blockchain performance is assessed by using transaction throughput and latency metric.

3.3 Performance of proposed and baseline comparison

In this section, the results obtained using the proposed Spatio-Temporal Attention-based Deep Learning (STA-DL) method are compared with those achieved using existing methods, including Multi-layer blockchain-based Decentralized Digital Identity (MDID) [1], Zero-trust for DDIM [2], and Self-Sovereign Digital Identity (SSDI) [3]. The outcome metrics used for comparative evaluation include transaction throughput, latency, fraud pattern detection accuracy, precision, and recall.

To ensure equivalent experimental conditions, all baseline methods [1], [2], and [3] were implemented, trained, and tested using the exact same software environment (Python version 3.10.11) and hardware configuration (Intel Core i7 processor, 8 GB RAM, 2 TB storage drive, and Windows 10 OS with GPU availability) as the proposed model, utilizing the common IDNet dataset.

Blockchain-related performance metrics, namely latency and transaction throughput, were measured explicitly. Latency in blockchain-powered digital identity frameworks denotes the time consumed between initiating an identity action (i.e., registration, feature extraction, and validation) and its final, immutable confirmation on the ledger. Transaction throughput denotes the rate at which identity evaluation along with cryptographic proofs are executed.

Furthermore, detection metrics (accuracy, precision, recall, and F1-score) were computed on the IDNet dataset. These measured values are presented in **Tables 3 through 6**. The results were determined by incrementing the sample size from 600 to 6,000. Analyzing these metrics across different sample sizes enables us to evaluate how each method responds to varying data scales for fraud pattern detection

3.4 Performance analysis of transaction throughput

As far as DDIM systems for fraud detection are concerned, the transaction throughput represents the rate at which identity evaluation along with cryptographic proofs are performed. It is measured in terms of transactions per second (TPS). By measuring the transaction throughput it helps is dictating how swiftly a user can be authenticated without delaying legitimate transactions. Table 3 lists the details of transaction throughput.

Table 3. Transaction throughput analysis using STA-DL, MDID[1], Zero-trust for DDIM [2] and SSDI [3]

Samples	Transaction throughput (TPS)			
	STA-DL	MDID [1]	Zero-trust for DDIM [2]	SSDI [3]
600	530	470	430	410
1200	940	820	780	760
1800	1460	1370	1330	1310
2400	1975	1815	1745	1725
3000	2475	2295	2260	2240
3600	2965	2715	2635	2615
4200	3465	2835	2755	2735
4800	4035	3725	3025	3005
5400	5035	4755	4015	3825
6000	5085	4835	4525	4205

Table 3 shows the transaction throughput evaluation using the proposed STA-DL and three existing methods, MDID [1], Zero-trust for DDIM [2] and SSDI [3]. The sample sizes or number of users used for the simulation are represented in Table 3. From the tabular representation, increasing the number of samples or users involved in fraud pattern detection process results in the increase in transaction throughput. This is because higher the number of samples more probability of fraud pattern detection process and vice versa. Also, simulation results show betterment of transaction throughput improvements using proposed STA-DL method upon comparison to [1], [2] and [3]. The reason is by applying the optimal threshold statistically separates the images from the metadata by maximizing variance between classes. This converts images into simple binary arrays, necessitating less processing capability, therefore creating a more streamlined authentication flow. With this the overall transaction throughput of proposed STA-DL method is found to be improved by 5.17% compared to [1], 12.38% compared to [2] and 20.93% compared to [3].

3.5 Performance analysis of latency

Latency in blockchain-powered digital identity frameworks denotes the time consumed between initiating an identity action (i.e. registration, feature extraction and validation) and its final, immutable confirmation on the ledger. It is measured in terms of seconds. This is mathematically formulated as given below.

$$Lat = Tuser + TFE + TPoW \tag{20}$$

From the above **equation (20)** latency'Lat' is measured by considering the time consumed in generating identifier'$Tuser$', time consumed to extract feature (i.e. image and meta data)'TFE', and finally the generation of proof of work '$TPoW$' respectively. Table 4 lists the details of latency.

Table 4 shows the latency measured in terms of seconds (sec) with respect to sample size ranging between 600 and 6000. The samples or users involved in simulation process are represented in Table 4. The latency involved in fraud pattern detection

Table 4. Latency analysis using STA-DL, MDID [1], Zero-trust for DDIM[2] and SSDI [3]

Samples	Latency(sec)			
	STA-DL	MDID [1]	Zero-trust for DDIM [2]	SSDI [3]
600	7.8	8.4	8.8	10.8
1200	8.3	9.4	9.8	10.2
1800	8.8	9.9	10.3	10.55
2400	9.15	10.16	10.2	10.85
3000	9.35	10.45	10.65	11
3600	9.85	10.95	11.25	11.45
4200	10.25	11.35	11.55	11.8
4800	10.55	11.65	11.85	12
5400	11	12	12.25	12.55
6000	11.35	12.45	12.65	13

with DDIM system is measured in seconds. From the above table, the latency using all the four methods was observed to be increasing with the increase in the sample size, therefore corroborating the objective of efficient fraud pattern detection in a significant manner. Also, the latency using proposed STA-DL method was found to be comparatively lesser than all the other three methods. The reason was by using the asymmetric encryption function along with optimal threshold based pre-processing in the proposed STA-DL method no single entity reconstructs the key, eliminating single points of failure. Moreover, incorporating asymmetric encryption function with optimal threshold based pre-processing minimizes the computation load making it heavily effective for fraud pattern detection. As a result, the latency of the proposed STA-DL method was found to be comparatively lesser by 8.84% compared to [1], 10.28% compared to [2] and 12.69% compared to [3].

3.6 Performance analysis of precision, recall, fraud detection accuracy

As far as DDIM system is concerned, precision evaluates the reliability of fraud flags (i.e. flagged users actually fraudulent), recall measures the methods ability to generate real fraud case and finally accuracy evaluates the overall correctness. This is mathematically defined as given below.

$$\text{Pre} = \frac{TP}{TP+FP} \tag{21}$$

$$\text{Rec} = \frac{TP}{TP+FN} \tag{22}$$

$$Acc = \frac{TP+TN}{TP+FP+TN+FNFN} \tag{23}$$

From the above **equations (21), (22) and (23)**, precision 'Pre', recall 'Rec' and accuracy 'Acc' is measured based on the true positive rate 'TP', false positive rate 'FP', true negative rate 'TN' and false negative rate 'FN' respectively. Table 5 given lists the details of precision, recall and fraud detection accuracy.

Table 5 shows the precision, recall and fraud detection accuracy using the four methods, STA-DL, MDID [1], Zero-trust for DDIM [2] and SSDI [3]. By measuring precision aids in preventing unauthorized access. To be more specific, if a DDIM system triggers a smart contract based on ID clearance via proof of work, high precision rate makes certain only the actual user of Decentralized Identifier (DID) gains access. By applying the proposed Spatial Temporal Attention-based Deep LSTM not only prioritizes but also isolates relevant metadata features in a dynamic fashion. This filtering straightforwardly minimizes false positives and aids in improving precision of proposed STA-DL method by 10% compared to [1], 13% compared to [2] and 17% compared to [3]. On the other hand, highly secure DID infrastructure prioritize high recall during identity document analysis to make certain that no forged digital credentials slip through. By understanding the sequential history of credential usage and authentication requests, the deep LSTM architecture learns normal user behavior over time. This condition distinctly minimizes false negatives and aids in boosting recall of proposed STA-DL method by 7% compared to [1], 8% compared to [2] and 12%

Table 5. Precision, recall and accuracy analysis using STA-DL, MDID [1], Zero-trust for DDIM [2] and SSDI [3]

Samples	Precision				Recall				Accuracy			
	STA-DL	MDID[1]	Zero-trust forDDIM[2]	SSDI[3]	STA-DL	MDID [1]	Zero-trust forDDIM[2]	SSDI[3]	STA-DL	MDID[1]	Zero-trust forDDIM[2]	SSDI[3]
600	0.97	0.96	0.95	0.94	0.99	0.98	0.98	0.98	0.96	0.95	0.94	0.93
1200	0.94	0.84	0.81	0.78	0.97	0.89	0.86	0.82	0.94	0.87	0.84	0.8
1800	0.92	0.82	0.79	0.76	0.96	0.88	0.85	0.81	0.92	0.85	0.82	0.78
2400	0.9	0.8	0.77	0.74	0.94	0.86	0.83	0.79	0.9	0.83	0.8	0.76
3000	0.88	0.78	0.75	0.72	0.92	0.84	0.81	0.77	0.87	0.8	0.77	0.73
3600	0.85	0.75	0.72	0.69	0.9	0.82	0.79	0.75	0.84	0.77	0.74	0.71
4200	0.83	0.73	0.7	0.67	0.88	0.85	0.82	0.8	0.82	0.75	0.72	0.68
4800	0.85	0.75	0.72	0.69	0.91	0.83	0.8	0.76	0.85	0.78	0.75	0.71
5400	0.88	0.78	0.75	0.72	0.93	0.85	0.82	0.78	0.88	0.81	0.78	0.74
6000	0.9	0.8	0.77	0.74	0.95	0.87	0.84	0.8	0.93	0.85	0.82	0.78

compared to [3]. Finally, by incorporating spatial attention map and temporal attention map results, the attention mechanism fine tunes metadata feature significance. This in turn generates robust, high-dimensional boundaries between legitimate users and malicious users. With this the overall accuracy of proposed STA-DL method is improved by 7% compared to [1], 11% compared to [2] and 15% compared to [3].

3.7 Overall performance analysis results

The overall performance result shows that the proposed STA-DL attained better performance when compared existing MDID [1], Zero-trust for DDIM[2]and SSDI [3] across multiple key metrics, including transaction throughput, latency, accuracy, precision and recall.

Table 6. Overall performance analysis results

Methods	Proposed STA-DL	Existing MDID [1]	Existing Zero-trust for DDIM[2]	Existing SSDI [3]
Transaction throughput (TPS)	2796.5	2563.5	2350	2283
Latency (sec)	9.64	10.67	10.93	11.32
Accuracy	0.891	0.826	0.798	0.762
Precision	0.892	0.801	0.773	0.745
Recall	0.935	0.867	0.84	0.806

Table 6 shows that overall performance results of all parameters for four methods namely proposed and compared existing [1] [2] and [3]. From the above table results, accuracy was obtained as 0.891, 0.826, 0.798 and 0.762 for STA-DL, MDID [1], Zero-trust for DDIM [2]and SSDI [3]. In addition, precision was attained as 0.892, 0.801, 0.773 and 0.745 by using STA-DL, MDID [1], Zero-trust for DDIM [2]and SSDI [3]. Also, recall was obtained as 0.935, 0.867, 0.84 and 0.806 for STA-DL, MDID [1], Zero-trust for DDIM [2]and SSDI [3]. Similarly, transaction throughput was found to be 2796.5 TPS, 2563.5 TPS, 2350 TPS and 2283 TPS for STA-DL, MDID [1], Zero-trust for DDIM [2]and SSDI [3]. Among the four methods, the proposed STA-DL outperforms the existing methods through reducing latency of 9.64sec, 10.67sec, 10.93sec and 11.32sec for the STA-DL, [1] [2] and [3]. These results indicate that the proposed STA-DL improved the decentralized digital identity management performance when compared to the other existing methods.

3.8 Statistical test

Paired t-test is Standardized Test Statistic for efficient decentralized digital identity management performance. It is also called as dependent samples t-test. Paired t-test is conducted for proposed STA-DL and the existing [1] [2] and [3] using IDNet dataset based on accuracy value.

In Table 7 and Figure 9, paired t-tests outcome is described. STA-DL achieved statistically significant improvements over [1], [2][3] with all p-values below 0.05. The highest t-statistic was observed for indicating the strongest performance difference. The paired t-test results show that STA-DL performed significantly better than all compared models.

Table 7. Paired t-test result for IDNet dataset (10 runs for sample size 600-6000 observations)

Comparison	Mean Difference	95% CI	t	df	p-value	p-value (Bonferroni)	Cohen's d	Significance
STA-DL vs MDID [1]	0.0650	[0.0510, 0.0790]	10.498	9	< 0.001	< 0.001	3.320	***
STA-DL vs Zero-trust for DDIM [2]	0.0930	[0.0745, 0.1115]	11.381	9	< 0.001	< 0.001	3.599	***
STA-DL vs SSDI [3]	0.1290	[0.1039, 0.1541]	11.621	9	< 0.001	< 0.001	3.675	***

Significance (Bonferroni adjusted): *** p < 0.001, ** p < 0.01, * p < 0.05, ns = not significant. n = 10 paired observations.

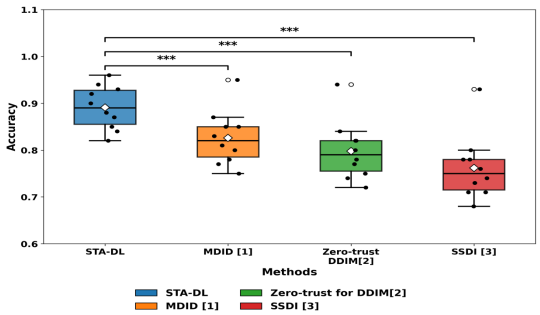

Fig 9. Paired t-tests Outcome for IDNet dataset

3.9 Threat model

The adversaries include a document forger who submits altered documents of the kinds found in the IDNet dataset (inpaint and rewrite, crop and move, face morphing, portrait substitution, text field replacement, or a mix of these), an impersonator who has stolen a user's credentials, a network attacker who intercepts or replays messages, and a malicious node that tries to change stored records. Each threat is handled by a different component. The STA-DLSTM model is the only defense against forged documents. The X.509 certificate and RSA signature prove who issued a report and that it has not been changed, while hash-linking with Proof-of-Work makes it computationally infeasible to alter a stored record later. We assume that private keys stay secret, that the cryptographic primitives (RSA-2048, SHA-256) are secure, and that honest nodes hold most of the mining power. Only signed metadata and report hashes are kept on the blockchain, while raw document images stay off-chain.

4 Conclusion

This study presented a novel DDIM method for fraud detection using Spatio-Temporal Attention-based Deep Learning (STA-DL) method by identity documents to facilitate privacy-preserving fraud detection. The proposed STA-DL method performs the tasks of registration, logic, feature extraction and validation for fraud pattern detection. With the collected identity documents, first registration process is applied to register and generate public and private key pairs. Followed by which feature extraction (i.e. from images and metadata) is performed by applying Spatial Temporal Attention-based Deep Long Short Term Memory model. Then the distinct fraud patterns and long-range relationships from digital identity documents are identified with improved transaction throughput and minimal latency. Finally using X509 as public key standard of cryptography validation is made with improved precision and accuracy. The algorithm is outlined to optimize five performance metrics, improving transaction throughput, latency, precision, recall and fraud detection accuracy. The proposed STA-DL method is assessed on various numbers of simulation runs. The performance of the proposed STA-DL method is compared to the DDIM system methods such as MDID, Zero-trust for DDIM and SSDI using different performance metrics. Experimental results prove that the proposed STA-DL method efficiently detects fraud patterns in a significant manner.

4.1 Quantitative Performance Comparison

The quantitative performance evaluation demonstrates the effectiveness of the proposed STA-DL framework in decentralized digital identity management. At the maximum evaluated sample size of 6,000, the proposed framework achieved an accuracy

of 0.93, precision of 0.90, and recall of 0.95 for fraud detection. It also attained a transaction throughput of 5085 TPS with a latency of 11.35 seconds. Furthermore, the overall average performance comparison presented in Table 6 shows that STA-DL achieved an average throughput of 2796.5 TPS and a latency of 9.64 seconds, compared with 2563.5 TPS and 10.67 seconds for MDID, 2350 TPS and 10.93 seconds for Zero-trust for DDIM, and 2283 TPS and 11.32 seconds for SSDI. Similarly, the proposed framework achieved average accuracy, precision, and recall values of 0.891, 0.892, and 0.935, respectively, outperforming the existing methods. These results highlight the effectiveness of integrating spatial-temporal attention-based deep learning with blockchain-assisted identity validation for improving fraud detection and decentralized digital identity management.

4.2 Scientific Contributions

The main scientific contribution of this research is the integration of spatial and temporal attention-based deep learning with blockchain-assisted decentralized digital identity management. The STA-DL architecture is designed to extract discriminative identity document features and identify potential fraudulent patterns. Furthermore, the incorporation of X.509 certificate-based verification and Proof-of-Work-based blockchain validation provides a combined mechanism for document-level fraud detection and decentralized identity verification. This integration distinguishes the proposed framework from approaches that primarily concentrate either on blockchain-based identity management or deep learning-based document analysis.

4.3 Limitations

Although the proposed framework demonstrates the potential of integrating deep learning-based fraud detection with blockchain-assisted identity management, certain limitations remain. The experimental evaluation is based on the IDNet dataset and the sample sizes considered in the study. Therefore, the generalizability of the framework requires further investigation using larger and more diverse real-world identity datasets. In addition, the computational requirements of attention-based feature extraction and blockchain transaction validation may introduce processing overhead. The scalability and deployment characteristics of the framework also require further evaluation in large-scale distributed environments.

4.4 Future Research Directions

Future research will focus on validating the proposed STA-DL framework using larger and more diverse real-world identity datasets. Further investigation will also examine methods for reducing computational overhead and improving the scalability of blockchain-assisted identity verification. In addition, the framework can be extended and evaluated in real-time deployment environments to examine its effectiveness under practical identity registration and authentication workloads.

References

1) Yu Q, Razali ASB, Salleh RB, Azzuhri SRB. MDID: a multi-layer blockchain-based secure and scalable decentralized identity scheme for web 3.0. *Journal of King Saud University Computer and Information Sciences*. 2026 Jan;38. Available from: https://link.springer.com/article/10.1007/s44443-025-00462-z.
2) Emati JHM, Tchendji VK, Djam-Doudou M. A zero-trust decentralized identifier specification based machine learning against cyber-attacks in blockchain based self-sovereign identity. *Journal of Cloud Computing*. 2026 Feb;15. Available from: https://link.springer.com/article/10.1186/s13677-026-00862-0.
3) Damasevicius R, Maskeliunas R. An analytical approach to blockchain-driven identity management in sustainable forest supply chains. *Supply Chain Analytics*. 2025 Dec;12. Available from: https://www.sciencedirect.com/science/article/pii/S2949863525000615.
4) Li Y, Yu B, Gao Y, Gao X, Zhang Y, Huang X, et al. RubberAIID: A lightweight intelligent platform for spatial localization and digital identification of individual rubber trees. *Smart Agricultural Technology*. 2026 Mar;13. Available from: https://www.sciencedirect.com/science/article/pii/S2772375526000924.
5) Dong Z, Tong W, Zhong A, Guo X, Xue L, Dong X. A Secure and Robust Blockchain-Based Identity Management Scheme Oriented to UAV Network. *Blockchain: Research and Applications*. 2026 Jan. Available from: https://www.sciencedirect.com/science/article/pii/S2096720926000011.
6) Deng J, Huang S, Han Q, Peng Z, Gu R, Li Y, et al. Blockchain-based Decentralized Identity Management for Cyber-Physical Systems Security. *Blockchain: Research and Applications*. 2026 Jun. Available from: https://www.sciencedirect.com/science/article/pii/S2096720926000722.
7) Fang J, Feng T, Guo X, Wang X. Privacy-enhanced distributed revocable identity management scheme based self-sovereign identity. *Journal of Cloud Computing*. 2024 Nov;13. Available from: https://link.springer.com/article/10.1186/s13677-024-00715-8.
8) Salem SHG, Hassan AY, Moustafa MS, Hassan MN. Blockchain-based biometric identity management. *Cluster Computing*. 2023 Nov;27. Available from: https://link.springer.com/article/10.1007/s10586-023-04180-x.
9) Chowdhury A. Vyoma commerce: a blockchain-based decentralized architecture to combat fraud and enhance security and trust in Bangladesh's e-commerce ecosystem leveraging smart contracts, supply chain transparency, and digital identity. *Journal of Electrical Systems and Information Technology*. 2025 Aug;12. Available from: https://link.springer.com/article/10.1186/s43067-025-00245-6.
10) Behbehani D, Komninos N, Muttukrishnan R. Sovchain: novel mutual authentication scheme for self-sovereign identity management using blockchain for open banking. *Journal of Cloud Computing*. 2026 Apr;12. Available from: https://www.researchgate.net/publication/403794436_Sovchain_novel_mutual_authentication_scheme_for_self-sovereign_identity_management_using_blockchain_for_open_banking.
11) Fathalla E, Azab M, Xin C, Wu H. Self-Sovereign Identity as a Secure and Trustworthy Approach to Digital Identity Management: A Comprehensive Survey. *ACM Computing Surveys*. 2026 Feb;58. Available from: https://share.google/Lg0Emf9aWeZ0aZY6K.

12) Ahmed MR, Islam AKMM, Shatabda S, Islam S. Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access*. 2022 Oct;10. Available from: https://ieeexplore.ieee.org/document/9927415.
13) Agarkar AA, Karyakarte M, Chavhan G, Patil M, Talware R, Kulkarni L. Blockchain aware decentralized identity management and access control system. *Measurement: Sensors*. 2024 Feb;31. Available from: https://www.sciencedirect.com/science/article/pii/S2665917424000084.
14) Suresh TD, Kumar RS, Bajaj M, Blazek V. A blockchain-enabled digital twin energy management framework for distributed optimization and secure peer-to-peer trading in DER-integrated microgrids. *Energy Reports*. 2026 Jun;15. Available from: https://www.sciencedirect.com/science/article/pii/S2352484726003367.
15) Zhang G, Hu Q, Zhang Y, Jiang T, Djam-Doudou M. A blockchain-based user-centric identity management toward 6G networks. *Digital Communications and Networks*. 2026 Jan. Available from: https://www.researchgate.net/publication/391886830.
16) Liu H, Cao J, Cao Y, Bai D, Liang J, Li R. EdenDID: an edge computing and blockchain-based decentralized identity system for Web3 applications and DePIN. *Cluster Computing*. 2025 Oct;28. Available from: https://link.springer.com/article/10.1007/s10586-025-05746-7.
17) Ouf S, Ahmed S, Helmy Y. A blockchain based deep learning framework for a smart learning environment. *Scientific Reports*. 2025 Jun. Available from: https://www.nature.com/articles/s41598-025-03688-z.
18) Kersic V, Vidovic V, Vrecko A, Domajnko M, Turkanovic M. Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. *IEEE Access*. 2023 Jul;11. Available from: https://ieeexplore.ieee.org/abstract/document/10194951.
19) Rathee T, Singh P. A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University - Computer and Information Sciences*. 2022 Sep;34. Available from: https://www.sciencedirect.com/science/article/pii/S1319157821000690.
20) Sutradhar S, Karforma S, Bose R, Roy S, Djebali S, Bhattacharyya D. Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain-based approach for security and scalability for healthcare industry. *Internet of Things and Cyber-Physical Systems*. 2023 Jul. Available from: https://www.sciencedirect.com/science/article/pii/S2667345223000470.
21) Yu H, Wang G, Dong A, Han Y, Wang Y, Yu J. Blockchain-enabled privacy protection scheme for IoT digital identity management. *High-Confidence Computing*. 2025 Dec;5. Available from: https://www.sciencedirect.com/science/article/pii/S2667295225000248.
22) Damaševičius R, Maskeliūnas R. An analytical approach to blockchain-driven identity management in sustainable forest supply chains. *Supply Chain Analytics*. 2025 Dec;12. Available from: https://www.sciencedirect.com/science/article/pii/S2949863525000615.
23) Qurashi MA. Decentralized Identity Management for Industrial Internet of Things Utilizing Blockchain-Enhanced Multi-Factor Authentication. *International Journal of Communication Networks and Applications*. 2024 Jul;11. Available from: https://www.ijcna.org/Manuscripts/IJCNA-2024-O-33.pdf.
24) Bochnia R, Richter D, Anke J. Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. *IEEE Access*. 2024 Jan;12. Available from: https://ieeexplore.ieee.org/document/10194951.
25) Zeydan E, Blanco L, Mangues-Bafalluy J, Arslan SS, Turk Y, Yadav AK. Blockchain-Based Self-Sovereign Identity: Taking Control of Identity in Federated Learning. *IEEE Open Journal of the Communications Society*. 2024 Aug;5. Available from: https://ieeexplore.ieee.org/document/10646364.