Blockchain and Machine Learning-Based Certificate Organization Framework: An Advanced Style to Organizational Credential Authentication

Premananda Sahu
School of Computer Science and Engineering, Lovely Professional University, Punjab, India
prema.uce@gmail.com

Saurabh Tembhurne
Master Trainer ,
Edunet Foundation ,Department of AI/ML
saurabhtembhurne8@gmail.com

Bhipinder Singh
School of Computer Science and Engineering, Lovely Professional University, Punjab, India
prema.uce@gmail.com

Sathish Krishna Anumula [0009-0009-0613-4863]
IBM Corporation ,
sathishkrishna@gmail.com

Umang
Department of Computer Applications,
DSB Campus, Kumaun University Nainital
anilumang@yahoo.co.in

Aldrin Manon
Dept. of CSE,
Uttaranchal Institute of Technology,
Uttaranchal University, Dehradun, India
aldrinmanon@uumail.in

***Abstract*— This paper proposes a robust agenda for certificate validation, enhancing security through the integration of ML and blockchain technologies. The system uses a machine learning agenda with two layers. The first model looks at the text parts of the certificate, such as ID, category of certificate, designation of the issuer and recipient, and the dates it was issued and will expire. The 2nd model forms the certificate's visual elements at the same time as the first one. Again, there is a cross-check that uses an OCR extract of the recipient's name and the metadata stored in the blockchain to make sure everything is correct. There are two main parts to the interface: "Issue Certificate" and "Verification." The "Issue Certificate" module lets users create novel digital certificates with metadata factors they choose. It also adds visual security features like signatures, logos, watermarks, and QR codes that are made in real time. The "Verification" module, on the other hand, uses IPFS and Pinata to store old or new certificates on the Sepolia test network in a way that makes them unchangeable and verifiable. This included the model provides a refined and adaptable solution to the challenges of issuing and validating certificates, addressing text security and forgery values for image & text files, while also safeguarding the certificates with blockchain technology to ensure their integrity. It works very well to make by inspection of digital certificates more trustworthy and open. The investigational results display a valid percentage rate of 96.88 %.**

Keywords— Certificate Validation, Blockchain, Machine Learning, Sepolia, OCR

I. INTRODUCTION

Today, it's likely that every organization needs to issue and verify various kinds of certificates to show that someone has done something or has certain skills. It is important for the management of these identifications to be both safe and effective. All of the old ways are manual, hefty, and stiff to keep fraud-free, which makes it harder to scale them up. To fill these openings, the paper proposes a novel organizational merit-based structure through a certificate management and authentication system that integrates blockchain technology and ML. This will most likely lead to a single solution: Work with the whole process, from issuing the certificates to checking them. All certificates delivered will have a exclusive hash that is verified and deposited using the blockchain technology's built-in security and changelessness. This guarantees their validity and stops interfering [1]. The system also uses two different specialized ML models to check the data. The first model would use the organized metadata that goes with each certificate, such as the recipient's name, the provider, the types of certificates, and the rationality periods, to set the basic rules for validating the certificate. The second model, on the other hand, focusses on the certificate's real visual veracity by using new methods for detecting interfering and mismatches/noncompliance in important parts like signatures, logos, watermarks, and embedded QR codes that carry the blockchain hash. Optical Character Recognition also matches the text on the certificate image with its metadata. The new predicted system will have a user-friendly interface for the people who work for the organization. One very exciting thing about the module is that it lets you add prevailing certificates to the system. Organizations can scan and upload their historical records, and the ML models will analyze them for probable artifacts. Validated preexisting certificates can then be linked with metadata, and hashed to the blockchain to bring them under the roof of the system for security management. Last but not the least, the system will facilitate the management of the credit/merit-based system, which is really an important thing for organizations since it has potential to link points or merit value with the certificates that are issued [2]. The "Verification" module will present a strong mechanism for verification of any certificate for the system, newly issued or older. All such certificates will have their blockchain records checked and will undergo analysis for both metadata and visual integrity based on ML for validation. The rest of this work has expressed in following manner: section II describes existing work, section III describes methods and techniques, section IV Performance evaluation and discussion, section V describes issue certificate and verification module, section VI describes conclusion and future scope followed by reference.

II. EXISTING WORK

Many researchers in the past have worked in the areas of certificate validation on the blockchain and document forgery detection through machine learning. These works create the groundwork toward a robust system integrating metadata validation, visual anomaly detection, and decentralized storage. A brief depiction of some of their work goes as follows:

T Rahman et al. [3] has proposed an academic credential verification system that operates on blockchain and IPFS with the aim of fighting against fake certificates in Southeast Asia. Certificates are hashed and stored on the IPFS, while the hash is recorded on the blockchain, allowing for tamper-proof verification. There should be ease of accessing verified credentials by employers- such a process being secure, cost-efficient, and fast, thereby cutting down on manual processes and fraud. A. Tariq et al. [4] have shown that Cerberus is a good way to check credentials on the blockchain-based credential verification mechanism to shelve a very common credential fraud. Cerberus is different from outdated methods because it works with existing confirmation ecosystems and uses on-chain smart indentures for cancelation rather than making users deal with personal information management. M. Ul Hassan et al. [5] have examined how anomaly recognition models provide blockchain applications with immediate detection of dubious actions. The function of anomaly detection in safeguarding blockchain applications is delineated with essential metrics and assessment criteria, succeeded by the classification of identification models across various blockchain layers. The paper finishes with existing challenges and research directions to take in developing reliable and secure blockchain systems.

DL Silaghi and DE Popescu [6] have shown that more people are into using blockchain for big schools, where some try out new ways to check if degrees are real. But these are just tests – they don't really stop fake degrees yet. Often, these efforts don't connect well with job systems for easy checks. Still, blockchain could really help keep clear, lifelong school records, which is super needed for school and work stuff. M. J. Rashmi et al. [7] has indicated that IDLSP system checks student papers automatically using smart tech like NLP and MLP. It looks at papers by taking in data, setting it up, and pulling out key parts to spot the real ones. With 92% right answers, it does better than others in being big, fast, and trustworthy. B Zhang et al. [8] have taken deep learning, a step further by making sure that the authors can forget stuff safely when needed, even with tricky DNN setups. It suggests a smart way to cut down on heavy math work but still keep safe checks. It also deals with training that doesn't settle and removing things step by step, for needs that keep changing. Tests on three sets of data show it works well and points out why forgetting safely in DNNs is good. D. Shah et al. [9] has indicated that their article digs into how blockchain and machine learning have grown during the sickness, especially in staying at home for work and school. It shows how much we depend on digital stuff now and points out problems like how people see it and not enough proper learning. CV Icociu et al. [10] has shown how blockchain and machine learning are changing education. Blockchain keeps school records safe and unchangeable. Machine learning helps plan out student growth with smart guesses. The paper talks about how together, these technologies could make school better and more honest, suggesting a future where safe data and smart planning improve how we learn and how well schools work and the certificate management process also.

III. METHODS AND TECHNIQUES

This work dealt with the construction of a machine-learning and blockchain-assisted certificate validation system. The system accommodates 3 machine-learning models like XGBoost Classifier for metadata validation, MobileNetV2 CNN for visualization of anomalies, and a computer-vision template-matching technique, with blockchain technologies such as Ethereum Sepolia testnet and IPFS (through Pinata) for secure storage and verification. The front end has two different modules: Certificate issuance and Certificate verification, thus forming a robust and user-friendly solution for ensuring authenticity. The total process that how the validation has done and what are the ML and Blockchain approaches are included to do this, has shown in Fig.1.

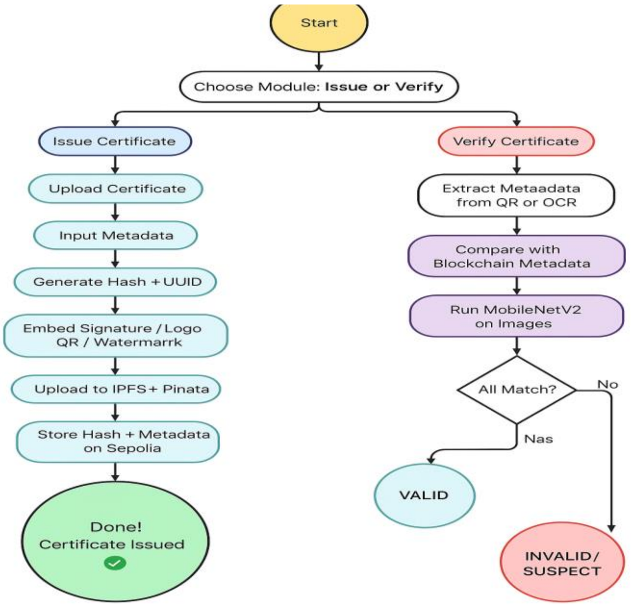

Start
Choose Module: Issue or Verify
Issue Certificate
Upload Certificate
Input Metadata
Generate Hash + UUID
Embed Signature / Logo QR / Watermarrk
Upload to IPFS+ Pinata
Store Hash + Metadata on Sepolia
Done! Certificate Issued
Verify Certificate
Extract Metaadata from QR or OCR
Compare with Blockchain Metadata
Run MobileNetV2 on Images
All Match?
No
Nas
VALID
INVALID/ SUSPECT

Fig.1. Overall Workflow Diagram

A. *XGBoost for Metadata Validation*

The XGBoost Classifier is key in checking data details. As a tuned boosting tool, XGBoost works well with organized data and finds small, often missed patterns in certificate info—like names, dates, where it's from, and signed bits. It checks that stuff like who gave it, student names, when it was given, QR links, and ID numbers are all correct. XGBoost builds a group of trees one by one, each new tree fixing the last one's mistakes by getting better bit by bit [11]. It gets trained on real and fake data, so it learns to spot the good from the bad really well. This check makes sure that any info in a certificate is right and fits what's usual, before it gets locked in the blockchain. This is the first smart step to stop messed-up or fake papers.

The above model has described objective function L(ϕ) as:

$$L(\emptyset) = \sum_{j=1}^{n} l\left(y_j, \hat{y}_j\right) + \sum_{t=1}^{T} \Omega\left(f_t\right) \quad (1)$$

Where,

Y_j is actual label, $\hat{y}_j$ is true label, $\Omega\left(f_t\right)$ is penalty for complex tree t and T is total number of trees.

The metadata becomes a clear feature vector X and the classifier gives a likelihood score which is referred as:

$$\hat{y} = P\,(valid|\,X) \quad (2)$$

Records with poor confidence get a flag for more checks or are not allowed on the blockchain. The model is great for this job because it deals with non-simple links and big feature mixes well. Also, XGBoost helps a lot – it uses methods like picking parts of columns, cutting trees, and sketching with weights for better size handling and quick work, really good for checking big groups of company proofs.

B. *MobileNetV2 CNN for Visualization of Anomalies*

MobileNetV2 is key in checking pictures. It spots weird things in digital or scanned document images. It's a CNN made for mobile stuff, good for spotting details in pictures without needing lots of power. It learns from real and changed documents. It gets what normal ones should have, like school symbols, okayed signatures, watermarks, QR stuff, and how they're set up. When someone gives a document to check, MobileNetV2 looks at it to find any wrong parts. Blurs, gaps, or changes are signs of messing with it [12]. This check works with other ways, like looking at data and using blockchain, to catch bad documents that could look okay in text or data alone. Using MobileNetV2 makes the whole checking process better, more reliable, and secure. It helps check documents well, fast, and a lot at once.

Finally, it detects the signs of tampering in visual elements-signatures, logos or hallmarks, watermarks, and QR codes encoding the hash-in images from certificates.

C. *Blockchain Technologies with Computer Vision Template Matching*

This approach Introduces a full and safe way to check digital certificates by using top tech like computer look, block storing, and spread-out file systems. One key part of this plan is using a look-based tech to match templates, which allows smart, auto checking of certificate images to spot any wrong bits or changes. Matching templates means looking at a scanned or uploaded certificate image with a set template kept safe on the system. This lets the system check if the picture design, things in it (like logos, QR codes, or signatures), and text features match well with the given certificate design. This strong method catches any changes or fakes like changed names, grades, or shape issues well, making the system really tough against document fraud [13].

To keep it all true, real, and safe from changes, the plan uses block tech through the Ethereum Sepolia test area, a safe and big area for using smart contracts. When a certificate is made, a crypto hash of its meta and visual info is made and kept on the Sepolia block. This unchangeable record makes sure that any later change to the certificate can be caught by comparing the now meta with the original hash kept on the block. The security network sends the genuine certificate and associated meta data to the Inter Planetary File System (IPFS), which is a way to store files across many computers. IPFS says that files will remain secure and straightforward to get to through unique content IDs (CIDs), and this are also linked to the block. This combination of IPFS and block adds a further layer of safety to make sure each of the ways gain and the truth of digital credentials. Overall, the combination of computer vision template matching and block-backed storage and verification really improves the trust and automation of methods for inspection organization certificates.

A threshold of 0.8 is set to determine a match, which could be presence or similarity in comparing certificate signatures and logos with genuine reference templates using OpenCV's `cv2.matchTemplate` with normalized cross-correlation.

D. *Training & Testing Process*

The data will be split into 80% for training and 20% for testing. Hyper-parameters have been optimized through grid search using Fitting 5 folds for each of 144 candidates, totaling 720 fits to maximize accuracy which has shown in Table I.

TABLE I. OPTIMIZATION OF HYPERPARAMETER VALUES

Hyperparameter	**Value**
classifier__colsample_bytree	0.8
classifier__learning rate	0.05
classifier__subsample	5
classifier__n_estimators	100
classifier__subsample	0.8

Application of altered signatures and blurred watermarks on the custom created certificates with a combination of rotation, scaling, and Gaussian noise enhancement in training process of the model. The model is trained with categorical cross-entropy loss, Adam optimizer (learning rate=0.001), and a batch size of 32.

E. *Algorithmic Structure of the proposed framework*

The structure has described in Fig. 2.

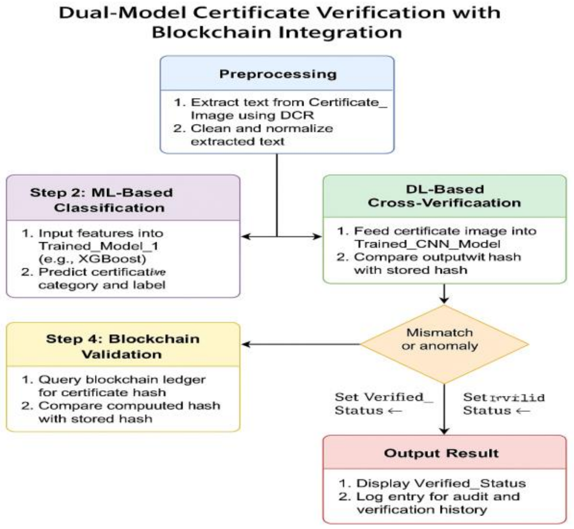

Dual-Model Certificate Verification with Blockchain Integration
Preprocessing
1. Extract text from Certificate_ Image using DCR
2. Clean and normalize extracted text
Step 2: ML-Based Classification
1. Input features into Trained_Model_1 (e.g., XGBoost)
2. Predict certificative category and label
DL-Based Cross-Verificaation
1. Feed certificate image into Trained_CNN_Model
2. Compare outputwit hash with stored hash
Mismatch or anomaly
Step 4: Blockchain Validation
1. Query blockchain ledger for certificate hash
2. Compare compuuted hash with stored hash
Set Verified_ Status ←
Set Irvilid Status ←
Output Result
1. Display Verified_Status
2. Log entry for audit and verification history

Fig.2. Proposed Algorithmic Structure

The flowchart shows a fusion of machine learning, deep learning, and blockchain on a certificate verification system. It includes preprocessing, ML classification, cross-validation with CNN and blockchain validation of hash functionality, which guarantees authenticity. The system clarifies assets or not through the evaluation that result to tested or invalid identities, which improve confidence, clarity and safety in online certificate authentication.

IV. PERFORMANCE EVALUATION AND DISC USSION

Here the authors have evaluated the performance of that certificate validation process based upon the above 3 types of methods used in the novel work.

Initially, 88% of the test data were classified correctly. The model showed a balanced performance across the valid and invalid certificate classes. For class 0 (valid), the precision was 0.82, recall of 0.89, and F1-score of 0.85; for class 1 (invalid), the precision was 0.91, recall of 0.85, and F1-score of 0.88. The overall macro and weighted averages of the performance were the same: precision, recall, and F1-score all at 0.88. During validation, metadata extracted from a certificate (using OCR or by manual input) are passed to the model and classified in binary as either valid or invalid, therefore ensuring the metadata conforms with defined expected patterns which has described in Fig.3.

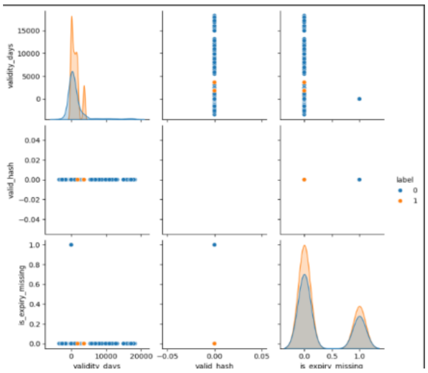


Fig.3. Pair Plot of Extracted Features of Metadata

The model may not generalize well as it works with exact matching, although this would be high precision. Thus, it can serve as a baseline for CNN's probabilistic approach [14]. This model confirms that expected visual elements are actually present during verification and serve as a complement (deterministic check) to the MobileNetV2 CNN [20-22]. Table II describes how visually the certificate validation has depicted.

TABLE II. CERTIFICATE VALIDATION COMPONENTS

Component	Details
Base Model	MobileNetV2 (pre-trained on ImageNet)
Input Image Size	224 × 224 × 3
Base Model Trainable	No (frozen during training)
Data Augmentation	Rotation (±10°), Zoom (±10%)
Rescaling	Yes (1./255) on all images
Additional Layers	GlobalAveragePooling2D → Dense (64, ReLU) → Dropout (0.3) → Dense (1, Sigmoid)
Loss Function	Binary Crossentropy
Optimizer	Adam
Metrics	Accuracy
Training Epochs	10
Batch Size	32
Class Mode	Binary
Training Directory	dataset/train
Validation Directory	dataset/val

Finally, while examining certificate images, the model would point out those specific areas that appear tampered with and cross-references it with the metadata to validate the text extracted from OCR [23-24]. Text (recipient name and further information) is extracted from images of certificates through Tesseract OCR, compared with other metadata, thus enriching itself for [25-29] further progress in the detection of anomalies. The model thus gives a score of 96.88% accuracy, judged against a confusion matrix [30] which has depicted in Fig.3 and metrics on anomaly detection rate, based on binary classification for each visual element, tampered/not-tampered has depicted in terms of ROC curve as Fig.4.

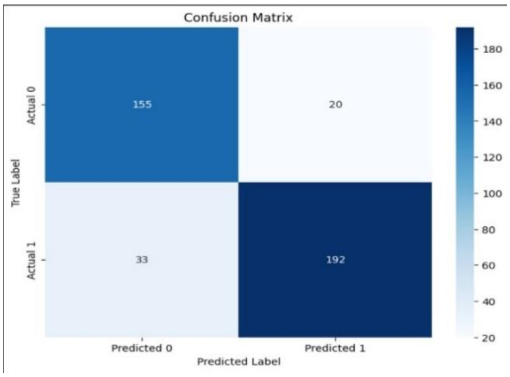


Fig.4. Confusion Matrix having Low FP

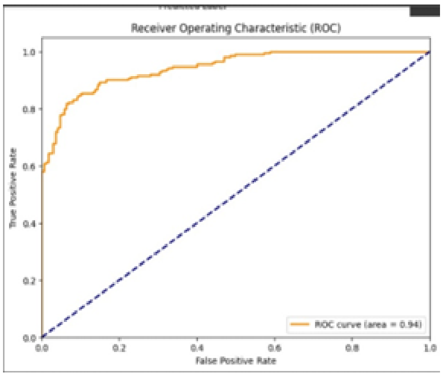


Fig.5. ROC with High TP and Low FP

V. CERTIFICATE ISSUE AND VERIFICATION

The certificates can be stored and verified in an immutable manner within the system using blockchain technology.

- ❖ The images of the certificates are uploaded to IPFS via Pinata. That way it is available decentralized and preserved forever. Metadata and SHA-256 hash from the image and metadata were stored using a smart contract in the Ethereum Sepolia test net.
- ❖ Written in Solidity, it manages the issuance of certificates and validation. It stores the hash, metadata, and CID relating to IPFS content. It has methods for adding certificates (Issue Certificate) and retrieving data (Verify Certificate).
- ❖ When a certificate is issued, it is uploaded onto IPFS, a hash is generated, and the smart contract records the data at the Sepolia testnet. Otherwise, during verification, the hash of the uploaded certificate is recomputed and compared with the chain record to check for alterations.
- ❖ Sepolia testnet, a cheap Ethereum test ground, provides immutability, and IPFS diversifies and makes it accessible.

A. Issue Certificate Module

This module enables issuers to create new certificates or complement already existing ones with security features and blockchain integration. Users fill out the metadata fields using forms (name, e.g., "recipient_name," "issuer_id"). A custom template will embed these fields onto the certificate image as text overlays (using, for example, Pillow to position, "certificate_id" at the top, "recipient_name" below). The following visual security elements will then be added: signature (digital or pre-stored), logo (issuer hallmark), watermark (semi-transparent pattern), and QR code (encoding the hash) [15-17].

A user uploads an already existing certificate image. Tesseract OCR extracts parallel text patterns from that (e.g. recipient name, dates) with a consistency check with user-provided metadata (e.g., using string if similar). If it is consistent, a watermark, logo, signature [18-19], and QR code will be overlaid on the image; if it is inconsistent, an exception will be flagged. Uploads the finalized certificate to IPFS using Pinata and records the metadata and hash on Sepolia Testnet. A template-based certificate downloadable with embedded security features and a blockchain record. For already existing certificates, the output is the enhanced image with overlaid elements and updated metadata.

B. Verification Module

The user verifies the certificate by uploading an image, which enables the performance of multi-layered authenticity checking:

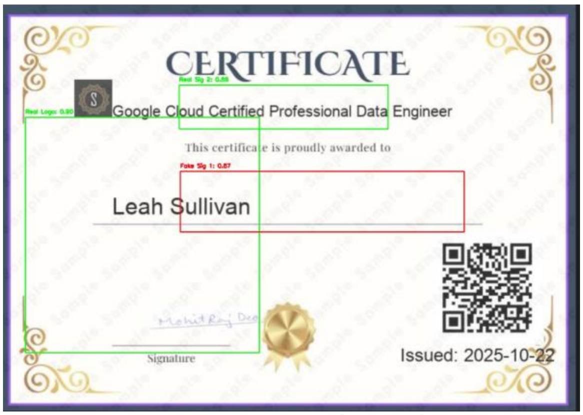
❖ The hash of the uploaded certificate is first calculated using SHA-256 and compared to the hash stored on the blockchain in Sepolia testnet.

❖ XGBoost Classifier (with 88% accuracy) analyzes the metadata extracted through OCR or manual methods for valid/invalid classification.

❖ Using a MobileNetV2 CNN and template-matching model, signatures, logos, watermarks, and QR codes will be assessed for the presence of tampering; the former gives an accuracy of 96.88%.

❖ A detailed report on authenticity, with tags for hash mismatches, inconsistencies in metadata, and evidence of visual tampering. In the case of pre-existing certificates, the results of verification would be based on comparison of the hash in the blockchain and alignment of OCR/metadata.

Now the template matching for a certificate has depicted in Fig.6.



CERTIFICATE

Google Cloud Certified Professional Data Engineer

This certificate is proudly awarded to

Leah Sullivan

Mohit Raj Deo

Signature

Issued: 2025-10-22

Fig.6. Template Matching

VI. CONCLUSION

It gives you an accurate, reliable and simple method to validate the certificates of your organization. By using top machine learning tech with split-up tech, the setup takes on big troubles like certificate fake, checking mistakes by hand, and no clear view in managing credentials. It mixes the XGBoost tool for checking data, MobileNetV2 CNN for seeing weird visuals, and a way to match layouts for steady look. It checks certificates deeply—both data and look. Plus, using blockchain through Ethereum's Sepolia testnet secures and tracks by saving hashed data, so no one can change records without getting caught. Using IPFS with Pinata for split-up storing makes it easy to reach and strong against losing data in one place. This two-way storing and checking make trust in checking credentials way stronger. The tests show this setup really catches changed or fake certificates well, while being easy and big enough for many users. It's great for schools, government, and companies that want to make their credential managing digital and safe. In short, mixing machine learning, blockchain, and computer seeing makes a new high in checking certificates, making sure things run smooth and with digital trust as more goes online and remote. A big chance to make it better is using advanced deep learning tech, like Vision Transformers or EfficientNet, for even better checks on small weird visuals or fakes. These techs, with special focus tools, could spot odd things in certificate images even better.

REFERENCES

[1] Y. Xie, W. Liu and Y. Wang, "A Traceable Cross-Domain Anonymous Authentication Scheme in Industrial Internet of Things," 2025 7th International Conference on Natural Language Processing (ICNLP), Guangzhou, China, 2025, pp. 679-684.

[2] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in *IEEE Access*, vol. 11, pp. 64679-64696, 2023.

[3] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-chain: A credentials verifier using blockchain and IPFS," in *Proc. Int. Conf. Inf., Commun. Comput. Technol.*, Singapore: Springer Nature Singapore, pp. 361–371, 2023.

[4] A. Tariq, H. Binte Haq and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," in *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1503-1514, Aug. 2023.

[5] M. Ul Hassan, M. H. Rehmani and J. Chen, "Anomaly Detection in Blockchain Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 289-318, Firstquarter 2023.

[6] D. L. Silaghi and D. E. Popescu, "A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions," *Computers*, vol. 14, no. 4, p. 141, Apr. 2025.

[7] M. J. Rashmi, N. V. Manoj Kumar, and K. Suguna, "Experimental evaluation of student certificate validation system using improved deep learning strategy with prediction principles," in *Proc. 5th Int. Conf. Image Process. Capsule Netw. (ICIPCN)*, Dhulikhel, Nepal, pp. 470–476, 2024.

[8] B. Zhang, Y. Dong, T. Wang, and J. Li, "Towards certified unlearning for deep neural networks," *arXiv preprint arXiv:2408.00920*, Aug. 1, 2024.

[9] D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, "Exploiting the capabilities of blockchain and machine learning in education," *Augmented Human Research*, vol. 6, pp. 1–4, Dec. 2021

[10] C. V. Icociu, C. I. Silvestru, and M. E. Lupescu, "Blockchain and machine learning: skills, competences and educational limitations," *Proc. Manuf. Syst.*, vol. 16, no. 4, pp. 143–149, 2021.

[11] A. Awasthi and N. Goel, "Phishing website prediction using base and ensemble classifier techniques with cross-validation," *Cybersecurity*, vol. 5, no. 1, p. 22, Nov. 2022.

[12] J. J. Pujari, T. Bikku, K. S. L. Prasanna, S. Kocherlakota, N. Gupta and R. Anitha, "Deepfake Image Verification using DCNN with MobileNetV2," *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, New Delhi, India, pp. 1-6, 2024.

[13] M. Ramalingam *et al.*, "A Comprehensive Analysis of Blockchain Applications for Securing Computer Vision Systems," in *IEEE Access*, vol. 11, pp. 107309-107330, 2023.

[14] P. Sahu, S. K. Mohapatra, U. Punia, P. K. Sarangi, J. Mohanty, and M. Rohra, "Deep learning techniques based brain tumor detection," in *Proc. 2024 11th Int. Conf. Reliability, Infocom Technol. Optim. (Trends Future Directions) (ICRITO)*, Noida, India, pp. 1–5, 2024.

[15] H. Gaikwad, N. D'Souza, R. Gupta, and A. K. Tripathy, "A blockchain-based verification system for academic certificates," in *Proc. 2021 Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Puducherry, India, pp. 1–6, 2021.

[16] S. Bharany and S. Sharma, “Intelligent green internet of things: An investigation,” in Machine Learning, Blockchain, and Cyber Security in Smart Environments, Chapman and Hall/CRC, 2022, pp. 1–15.

[17] K. Joshi, S. Bharany*et al., “Exploring the Connectivity Between Education 4.0 and Classroom 4.0: Technologies, Student Perspectives, and Engagement in the Digital Era,” IEEE Access, vol. 12. Institute of Electrical and Electronics Engineers (IEEE), pp. 24179–24204, 2024. doi: 10.1109/access.2024.3357786.

[18] A. Pundir *et al.*, "Enhancing gait recognition by multimodal fusion of mobilenetv1 and xception features via PCA for OaA-SVM classification," *Scientific Reports*, vol. 14, p. 17155, 2024, doi: 10.1038/s41598-024-68053-y.

[19] A. Bhardwaj *et al.*, "Proactive threat hunting to detect persistent behaviour-based advanced adversaries," *Egyptian Informatics Journal*, vol. 27, p. 100510, 2024, doi: 10.1016/j.eij.2024.100510.

[20] S. Bharany and M. Maashi, "A Critical Investigation into the Blockchain Technology and Its Present-Day Uses," in *Proc. 2023 3rd Int. Conf. Computing and Information Technology (ICCIT)*, Tabuk, Saudi Arabia, 2023, pp. 69–72, doi: 10.1109/ICCIT58132.2023.10273943.

[21] S. Bharany, S. Alam, M. Shuaib, and B. Talwar, "Sentiment Analysis of Twitter Data for COVID-19 Posts," in *Algorithms for Intelligent Systems*, Springer, Singapore, pp. 457–466, Dec. 2022, doi: 10.1007/978-981-19-6004-8_37.

[22] D. Somwanshi, A. Jain, K. Joshi, V. Kant, S. Bharany, and B. V. Kumar, “Advanced Face Detection Using SVM and Haar-like Features: A Comprehensive Approach in AI and Image Processing,” 2025 3rd International Conference on Advancement in Computation &amp;amp; Computer Technologies (InCACCT). IEEE, pp. 72–77, Apr. 17, 2025. doi: 10.1109/incacct65424.2025.11011443.

[23] S. Bharany *et al.*, "Wildfire Monitoring Based on Energy Efficient Clustering Approach for FANETS," *Drones*, vol. 6, no. 8, p. 193, Aug. 2022, doi: 10.3390/drones6080193.

[24] S. Bharany *et al.*, "A Systematic Survey on Energy-Efficient Techniques in Sustainable Cloud Computing," *Sustainability*, vol. 14, no. 10, p. 6256, May 2022, doi: 10.3390/su14106256.

[25] A. Godavarty, S. Rodriguez, Y.-J. Jung, and S. Gonzalez, "Optical imaging for breast cancer prescreening," *Breast Cancer Targets Ther.*, vol. 7, pp. 193–209, 2015.

[26] A. Jain, D. Somwanshi, C. Bhatt, A. Chaturvedi, H. Anandaram and K. Joshi, "Breast Cancer Diagnosis using Convolutional Neural Network," *2024 International Conference on IoT, Communication and Automation Technology (ICICAT)*, Gorakhpur, India, 2024, pp. 441-445, doi: 10.1109/ICICAT62666.2024.10922877.

[27] R. Kumari, K. Kaur, A. Almogren, A. Altameem, Y. Y. Ghadi, and A. U. Rehman, “C-BIVM: A Cognitive-Based Integrity Verification Model for IoT-Driven Smart Cities,” *Computers, Materials & Continua*, vol. 0, no. 0, pp. 1–10, 2025, doi: 10.32604/cmc.2025.064247.

[28] M. Malhotra, I. Chhabra, *et al*., “Examining the landscape of proctoring in upholding academic integrity: a bibliometric review of online examination practices,” *Discover Education*, vol. 4, p. 227, 2025, doi: 10.1007/s44217-025-00661-w.

[29] V. K. Mishra, M. Mishra, S. Saini, and S. Bharany, *et al*., “Exploiting Machine Learning for Vulnerable Road Users’ Protection of Moving Objects on Trajectory Motion: Dealing with Action Transformation Using AI Agent-Based Technologies,” *Arabian Journal for Science and Engineering*, 2025, doi: 10.1007/s13369-025-10346-z.

[30] A. Paul, I. Ganguli, R. S. Bhowmick, S. Badotra, S. Bharany, and A. U. Rehman, “DRL Based Traffic Signal Control Method Featuring Masked Approach to Redress Transmission Error in ITS,” *International Journal of Intelligent Transportation Systems Research*, 2025, doi: 10.1007/s13177-025-00482-z.