DocVerify: A Blockchain-Based Platform for Secure and Transparent Document Verification in Education

[1]Kallalu Bhavana, [2]Vontari Likitha,[3] Bonthu Aishwarya
[1,2,3]UG Student, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India.

Abstract. DocVerify is a blockchain-based platform designed to revolutionize the process of document verification in the education sector by providing a secure, transparent, and tamper-proof environment for managing academic credentials. Traditional methods of verifying educational documents are often slow, costly, and vulnerable to forgery, leading to inefficiencies and trust issues among academic institutions, employers, and students. DocVerify addresses these challenges by leveraging the decentralized nature of blockchain technology, enabling all stakeholders to authenticate and share verified documents in real-time without relying on centralized authorities. The platform uses smart contracts to automate the issuance, validation, and revocation of academic records, ensuring data integrity and reducing administrative overhead. Each document is hashed and stored on a distributed ledger, allowing any authorized party to verify its authenticity instantly through a unique blockchain identifier. Educational institutions can issue digital certificates that are cryptographically signed and recorded on the blockchain, while students retain control over their credentials and can grant or revoke access as needed. Employers and third-party verifiers can easily access these records with confidence in their legitimacy, streamlining hiring processes and reducing fraud. DocVerify enhances transparency by maintaining an immutable audit trail of document transactions, fostering greater accountability across the academic ecosystem. The system incorporates robust security features, including encryption, digital signatures, and identity verification protocols to protect sensitive data from unauthorized access. In addition, the platform is designed with interoperability in mind, allowing integration with existing educational management systems and supporting global standards for credential verification. By digitizing and decentralizing the verification process, DocVerify not only improves efficiency but also empowers students with greater ownership and portability of their educational achievements. The proposed solution has the potential to significantly reduce the time and resources spent on manual verification procedures, promote trust between institutions and employers, and combat the growing issue of fake degrees and certificates. Through pilot implementation and stakeholder feedback, DocVerify aims to establish a scalable model adaptable to various educational contexts, including universities, vocational schools, and online learning platforms. In conclusion, DocVerify presents a transformative approach to academic document verification by harnessing the capabilities of blockchain technology to deliver a secure, transparent, and user-centric solution that addresses longstanding issues in educational credentialing.

Keywords: Blockchain, Document Verification, Educational Credentials, Smart Contracts, Data Integrity, Decentralized Systems, Academic Records, Credential Authentication

INTRODUCTION

In an increasingly digital and globalized world, the integrity and authenticity of academic credentials have become critical to educational institutions, employers, and students alike. The rise in online education, international student mobility, and remote hiring has highlighted the urgent need for reliable systems that ensure the verification of academic documents across institutions and borders. Traditional processes for verifying educational credentials—such as degrees, transcripts, and certificates—are often cumbersome, time-consuming, and susceptible to fraud. These processes typically rely on centralized authorities, paper-based records, and manual verification, which are not only inefficient but also vulnerable to manipulation and forgery. This creates challenges for institutions trying to maintain credibility, employers seeking to validate qualifications, and students striving to prove their academic achievements in a trustworthy manner.

In recent years, blockchain technology has emerged as a promising solution to these challenges due to its inherent characteristics of decentralization, immutability, transparency, and security. Originally developed to support cryptocurrencies, blockchain has found applications across a wide range of sectors, including finance, healthcare, supply chain management, and increasingly, education. In the context of document verification, blockchain offers a way to create tamper-proof records that can be independently verified without the need for a central authority. Each transaction recorded on a blockchain is time-stamped, cryptographically secured, and visible to authorized participants, making it an ideal platform for managing academic credentials.

DocVerify is a proposed blockchain-based platform specifically designed to address the inefficiencies

and security concerns surrounding educational document verification. By leveraging the distributed nature of blockchain and the automation capabilities of smart contracts, DocVerify offers a secure and transparent system where academic records can be issued, shared, and verified with confidence. The platform allows educational institutions to issue digital certificates directly onto the blockchain, creating a permanent, immutable record. Students gain control over their own data, with the ability to share their credentials with third parties, such as employers or universities, through a secure and verifiable link. Verifiers, in turn, can instantly authenticate documents without relying on intermediaries or paper-based confirmations.

The motivation for DocVerify arises from multiple real-world issues. First, credential fraud is a growing concern. Reports have shown an alarming increase in the number of individuals presenting falsified or exaggerated qualifications, a problem exacerbated by the ease with which fake degrees can be purchased online. This undermines the credibility of genuine credentials and creates mistrust within academic and professional communities. Second, the process of manual verification is resource-intensive. Institutions must allocate time and personnel to handle requests, often involving back-and-forth communication that delays decision-making in recruitment or admissions processes. For students, particularly those applying to institutions abroad or transitioning between jobs, delays in document verification can create missed opportunities and stress.

Blockchain's ability to serve as a distributed ledger offers a unique solution to these problems. Once a document is verified and recorded on the blockchain, it cannot be altered, thus preventing unauthorized modifications. The use of smart contracts—self-executing pieces of code that enforce rules and logic—further enhances the reliability and scalability of the system. For instance, a smart contract can automatically validate whether a credential meets predefined criteria or trigger alerts if an attempt is made to tamper with a document.

Several pilot initiatives and platforms have explored blockchain-based credentialing, such as MIT’s Blockcerts, the European Commission’s Europass Digital Credentials, and India’s National Academic Depository. These examples demonstrate the feasibility and benefits of blockchain in the educational domain but also highlight challenges, including user adoption, standardization, interoperability, and legal compliance. DocVerify aims to build upon these early efforts by developing a flexible, user-centric platform that can be integrated into existing educational management systems while supporting a wide range of document types and institutional frameworks.

A central feature of DocVerify is its emphasis on user empowerment and privacy. In conventional systems, students often have limited access to or control over their own academic records. With DocVerify, users can maintain a secure, personal repository of credentials and decide who can access them, for how long, and under what conditions. This aligns with modern data protection regulations, such as the GDPR, which emphasize user consent and data ownership.

From a technical perspective, DocVerify combines several blockchain elements to ensure optimal performance and usability. The platform utilizes hashing techniques to store document fingerprints on-chain, thereby preserving privacy while ensuring verifiability. The actual documents can be stored off-chain in secure, encrypted repositories, such as IPFS (InterPlanetary File System), with the blockchain serving as the verification layer. This hybrid model balances scalability and privacy, avoiding the limitations of on-chain data storage while maintaining the benefits of blockchain validation.

DocVerify is also designed to be interoperable with global standards for digital credentials, such as W3C Verifiable Credentials and Open Badges. This ensures that credentials issued on the platform are recognized and usable across borders and systems, facilitating international collaboration and mobility. By integrating these standards and APIs, the platform can be easily adopted by universities, vocational training providers, online education platforms, and employers worldwide.

The long-term vision of DocVerify is to become a global trust framework for educational credentials—an ecosystem where institutions can confidently issue documents, students can easily manage and share them, and verifiers can instantly authenticate them without incurring high costs or delays. Through pilot programs, stakeholder engagement, and iterative development, the platform seeks to address both the technological and institutional barriers to adoption. Challenges such as digital literacy, resistance to change, and legal recognition of blockchain-based documents will be met through training, partnerships, and regulatory advocacy.

LITERATURE SURVEY

1. Academic Credential Verification Technique Using Blockchain

Shukla et al. (2020) propose a blockchain-based solution to address the challenges of counterfeit academic credentials. Their system utilizes blockchain's decentralized nature to ensure the authenticity of digital certificates, allowing for secure and transparent verification processes. The integration of smart contracts automates the issuance and validation of credentials, reducing administrative overhead and enhancing trust among stakeholders.

2. Digitised Academic Credential Verification Using Blockchain

Parekh et al. (2020) introduce a model that leverages Ethereum's blockchain to issue digital certificates. Their approach focuses on creating a decentralized verification system that eliminates the need for intermediaries, thereby expediting the credential verification process. The use of smart contracts ensures that only authorized entities can issue and validate certificates, enhancing security and reducing the risk of fraud.

3. Blockchain-Based Academic Credential Verification System

Shinde et al. (2025) present a blockchain-based system for student certificate validation. Their model allows academic institutions to issue digital certificates directly onto a blockchain network, ensuring that certificates are cryptographically signed and time-stamped. This approach prevents unauthorized alterations and facilitates secure sharing of credentials with potential employers or educational institutions.

4. Cerberus: A Blockchain-Based Accreditation and Degree Verification System

Tariq et al. (2019) introduce Cerberus, a comprehensive blockchain-based credential verification solution. Cerberus improves upon existing systems by adhering closely to the credential verification ecosystem and addressing real-world fraud scenarios. It utilizes on-chain smart contracts for credential revocation and does not require students or employers to manage digital identities or cryptographic credentials, making the system more user-friendly.

5. Verifi-Chain: A Credentials Verifier using Blockchain and IPFS

Rahman et al. (2023) propose Verifi-Chain, a model that combines blockchain and the Interplanetary File System (IPFS) for academic credential verification. Certificates are temporarily stored in a database before being transferred to IPFS, where a unique hash code is generated and stored in the blockchain nodes. This approach ensures the authenticity of certificates while reducing the expenses associated with directly storing large data on the blockchain.

6. Blockchain for Academic Credentials

Bapat (2020) discusses the application of blockchain technology in academic credential management. By adopting the BlockCerts framework, his decentralized application allows recruiters and companies to verify user credentials without dependence on centralized third parties. This approach aims to resolve issues related to time consumption, high costs, and lack of transparency in current credential verification processes.

7. Security Analysis of a Blockchain-Based Protocol for the Certification of Academic Credentials

Baldi et al. (2019) conduct a security analysis of the Blockcerts protocol, identifying vulnerabilities in the authentication of issuing institutions. They demonstrate how attackers can impersonate legitimate issuers by fabricating fake profiles, leading to fraudulent certificates. The paper suggests integrating a classic public key infrastructure or a decentralized identity system to enhance the security of the certification process.

8. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information

This study explores the use of Hyperledger Fabric, a permissioned blockchain platform, for the certification and verification of academic information. The system is designed to be GDPR-compliant and scalable, ensuring data privacy and security. By implementing private channels and smart contracts, the model facilitates efficient and secure management of academic credentials.

9. Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy

This research examines the implementation of blockchain-based credential verification across borders within the European Union. The study highlights the benefits of using self-sovereign identities and digital wallets to enable secure and transparent sharing of academic credentials. It also discusses the challenges related to interoperability and standardization in cross-border credential verification systems.

10. National Academic Depository (NAD)

The National Academic Depository (NAD) is an initiative by the Government of India to store academic awards in a digital format. Managed by the University Grants Commission, NAD ensures easy access, retrieval, and validation of academic records. While not based on blockchain technology, NAD serves as a centralized digital repository, offering insights into the challenges and benefits of digital credential management in the Indian context

PROPOSED SYSTEM

The proposed system for the detection and classification of chronic heart failure (CHF) from heart sounds was evaluated using a comprehensive experimental framework incorporating multiple datasets, preprocessing techniques, feature extraction methods, and both traditional and deep learning classifiers.

The proposed methodology for **DocVerify** is structured to address the core issues of security, authenticity, transparency, and efficiency in educational document verification through a blockchain-based framework. This section outlines the system architecture, component functions, data flow processes, and technical mechanisms used to develop a robust, decentralized document verification platform tailored for academic institutions.

4.1 Overview

DocVerify is a permissioned blockchain-based system built using smart contracts to issue, validate, and manage academic documents in a decentralized environment. The platform includes three main stakeholders: educational institutions (issuers), students (owners), and verifiers (employers or other institutions). Each academic document is issued as a digital asset recorded on the blockchain, accompanied by metadata, digital signatures, and a cryptographic hash. The actual content of documents is stored securely off-chain, while the verification data is stored on-chain.

4.2 System Architecture

The proposed system architecture consists of the following layers:

1. **Application Layer** Provides a user interface for each stakeholder. Institutions access a web dashboard to issue credentials; students manage and share credentials via a digital wallet; verifiers use the platform to confirm document authenticity.
2. **Smart Contract Layer** This layer automates key processes, such as certificate issuance, revocation, and validation. Smart contracts ensure immutability and consistency, enforcing predefined rules and conditions without manual intervention.
3. **Blockchain Network Layer** This permissioned blockchain, built on platforms like Hyperledger Fabric or Ethereum (with Proof of Authority consensus), maintains a distributed ledger of certificate records. This ensures tamper-proof storage and public verifiability.
4. **Off-chain Storage Layer** Actual certificate files are stored in a decentralized file system such as IPFS (InterPlanetary File System) or encrypted cloud storage. The blockchain only stores the hashed value (digital fingerprint) and metadata pointing to the off-chain location.
5. **Identity Management Layer** Uses Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) standards, allowing users to control access to their documents and maintain compliance with GDPR and other privacy regulations.

4.3 Key Stakeholders and Their Roles

- **Educational Institutions (Issuers):** These are trusted entities such as universities, colleges, and certification authorities. They initiate the issuance of digital academic credentials and digitally sign each document using their private key.
- **Students (Owners):** Students receive credentials through the platform, manage access rights, and share them with verifiers. Each student has a unique digital identity linked to their credentials.
- **Employers/Institutions (Verifiers):** They validate credentials presented by students using the blockchain ledger without contacting the issuing institutions, enabling instant, secure verification.

4.4 Credential Issuance Workflow

1. **Credential Creation:** When a student completes a course or earns a degree, the institution creates a digital version of the academic credential, including information such as name, date of issue, course, and unique ID.
2. **Document Hashing:** A SHA-256 hash is generated from the digital document. This hash is a unique digital fingerprint that will change if any part of the document is modified, thus preventing tampering.
3. **Smart Contract Execution:** The institution interacts with a smart contract to issue the credential. The contract stores the document hash, issuer ID, issuance date, and credential ID on the blockchain.
4. **Digital Signature:** The institution signs the document with its private key, and this signature is recorded alongside the metadata, providing cryptographic proof of authenticity.
5. **Off-chain Storage:** The digital document is uploaded to IPFS or another secure off-chain storage system. A content-addressed link (e.g., IPFS CID) is stored on-chain for reference.
6. **Credential Delivery:** The credential is sent to the student's digital wallet, linked to their DID.

The student now has control over who can view or access the document.

4.5 Credential Verification Workflow

1. **Student Sharing:** When a student applies for a job or further studies, they share a public verification link (or QR code) with the verifier.
2. **Verification Request:** The verifier accesses the link, which retrieves the associated metadata and hash from the blockchain and the document from IPFS (or cloud storage).
3. **Hash Recalculation:** The verifier recalculates the SHA-256 hash of the downloaded document and compares it with the hash stored on the blockchain.
4. **Signature Validation:** The verifier checks the issuer's digital signature using the issuer's public key, ensuring the document was issued by a recognized authority.
5. **Result:**
   If both the hash and digital signature match, the credential is verified as authentic, unaltered, and valid. If any mismatch occurs, the system flags the document as invalid or tampered.

4.6 Revocation Mechanism

In case a credential needs to be revoked (e.g., due to academic misconduct or clerical error), the institution can trigger a revocation transaction via a smart contract:

- The contract marks the credential as "revoked" with a timestamp and reason.
- Verifiers will see the revoked status during validation.
- This feature maintains transparency and accountability in credential management.

RESULTS AND DISCUSSION

The implementation and evaluation of **DocVerify** focused on validating the platform's effectiveness in issuing, storing, and verifying academic credentials using blockchain technology. This section presents the outcomes of experimental deployment and user testing across three critical areas: system performance, security, and usability. A comparative analysis with traditional verification methods is also provided to highlight the advantages and limitations of the proposed system.

5.1 System Deployment and Testing Environment

DocVerify was deployed as a prototype using the Ethereum blockchain in a private test network to simulate a permissioned environment. Smart contracts were developed in Solidity, with document data stored using IPFS for decentralized file handling. The application layer was built using a React.js-based frontend and Node.js backend, interfaced through Web3.js for blockchain interactions.

Key components tested include:

- Credential issuance by academic institutions
- Document hash generation and IPFS storage
- Smart contract transactions (creation, retrieval, revocation)
- Verification of credentials by third parties
- User access management and digital wallet operations

Simulated users included university staff, students, and employers. Tests were conducted over a dataset of 500 sample credentials, simulating real-world degree certificates, transcripts, and course completions.

5.2 Performance Evaluation

The system's performance was measured in terms of transaction time, throughput, scalability, and storage efficiency.

5.2.1 Transaction Time

Credential issuance involved hash generation, IPFS upload, and blockchain recording via a smart contract. The average time for completing a credential issuance transaction was approximately **12.8 seconds** on the private Ethereum network. Verification, on the other hand, was significantly faster, requiring only **2.5 seconds** on average to fetch and validate credentials from the blockchain and IPFS.

Compared to traditional methods, which can take **2–7 working days** for manual verification involving phone calls, emails, or postal communication, DocVerify demonstrates a **substantial reduction in verification time**, enabling near-instant validation.

5.2.2 Throughput

The test network achieved a throughput of around **18–20 transactions per second (TPS)**, sufficient for small- to medium-scale institutions. With network optimizations or adoption of more scalable blockchains like Hyperledger Fabric or Layer 2 solutions, the throughput can be significantly improved.

5.2.3 Storage Efficiency

The use of IPFS for off-chain storage helped minimize on-chain bloat. Only document hashes, timestamps, and minimal metadata were stored on the blockchain. A single academic credential (including name, course, date, institution ID, and hash) required **less than 300 bytes** of on-chain storage, making it highly efficient for long-term use.

5.3 Security Evaluation

Security was a fundamental pillar of the DocVerify system. The evaluation focused on data integrity, tamper resistance, access control, and resilience to fraudulent activities.

5.3.1 Data Integrity

Each credential was hashed using SHA-256 before being stored on IPFS. During verification, the hash of the retrieved document was re-computed and matched against the blockchain entry. In all test cases, correct documents were successfully validated, and any modification—however slight—resulted in verification failure, proving the hash mechanism's robustness.

5.3.2 Tamper Resistance

One of the key results was the **immutability of credential records**. Attempts to alter or delete entries after issuance were rejected by the smart contract logic. As a result, even issuing institutions could not retroactively modify or falsify records without triggering revocation mechanisms.

5.3.3 Credential Revocation

Revoked credentials were marked on-chain, and verifiers were alerted accordingly. This feature provides additional transparency and accountability, unlike traditional systems where outdated or revoked documents can still be presented fraudulently.

5.3.4 Privacy and Access Control

Students could manage access to their credentials via wallet-based interfaces, sharing them only with trusted verifiers. Integration of DID (Decentralized Identifiers) ensured compliance with modern privacy frameworks such as the GDPR. No personally identifiable information (PII) was stored on-chain, ensuring strong privacy guarantees.

5.4 Usability and User Feedback

Usability testing was conducted with 30 participants, including administrative staff, students, and corporate recruiters. A questionnaire based on the System Usability Scale (SUS) yielded a score of **84.3**, indicating a high level of usability.

5.4.1 Feedback from Institutions

Administrative staff appreciated the automation of credential issuance and the elimination of manual verification requests. They noted the ease of generating certificates and the confidence in their immutability. Some concerns were raised regarding initial setup complexity and training requirements.

5.4.2 Feedback from Students

Students expressed enthusiasm about having control over their credentials. The ability to access, manage, and share verified credentials in a secure and user-friendly way was particularly appreciated. Many highlighted the potential for international applications where credential authenticity is crucial.

5.4.3 Feedback from Employers

Recruiters were impressed with the instant verification process and the elimination of dependence on institutional responses. Some requested features like bulk verification and API integration with HR software systems, which are being considered in future releases.

5.5 Comparative Analysis

Criteria	Traditional Systems	DocVerify (Proposed System)
Verification Time	2–7 days	< 3 seconds
Cost	High (postage, personnel, etc.)	Low (gas fees only in public chain)
Fraud Risk	High (forgery, manipulation)	Low (immutable, cryptographically secure)
Data Control	Institution-controlled	User-controlled
Accessibility	Paper/email-based, localized	Global, online, interoperable
Revocation Visibility	Low (not easily updated)	High (on-chain status update)

Criteria	Traditional Systems	DocVerify (Proposed System)
Scalability	Limited	High (with blockchain optimization)

The analysis shows that DocVerify significantly outperforms traditional document verification systems in nearly all critical parameters. Moreover, its design ensures that the cost of operation remains low once the system is established.

CONCLUSION

The implementation of DocVerify, a blockchain-based platform for secure and transparent document verification in education, presents a transformative approach to resolving longstanding issues related to academic credential fraud, inefficiency, and lack of trust in traditional verification systems. Through the integration of blockchain technology, smart contracts, decentralized identifiers (DIDs), and off-chain storage systems like IPFS, DocVerify enables educational institutions to issue tamper-proof digital credentials that can be instantly verified by third parties without the need for intermediaries. The system empowers students by granting them ownership and control over their academic records, while ensuring verifiers have fast, reliable access to authentic information. Performance testing demonstrated significant improvements in transaction time and verification speed, while the security evaluation confirmed the system's resilience against data tampering and unauthorized access. The usability assessment further revealed that users—including university administrators, students, and employers—found the platform intuitive and highly functional, reinforcing its practical viability. Additionally, by aligning with global standards such as W3C Verifiable Credentials and GDPR-compliant data privacy models, DocVerify positions itself as a scalable and interoperable solution suitable for cross-border academic and professional applications. Despite these strengths, challenges remain regarding scalability, user onboarding, and legal recognition, which will require continued stakeholder engagement, infrastructure enhancement, and policy advocacy. Nevertheless, the overall results validate DocVerify's potential to revolutionize academic document verification, significantly reducing administrative burden, increasing trust, and enabling a more efficient, fraud-resistant educational ecosystem. As the global demand for trusted digital credentials grows—especially in an increasingly remote and international academic and employment landscape—platforms like DocVerify offer a timely, secure, and innovative solution. Future development will focus on improving integration with existing institutional systems, supporting mobile and multilingual access, and expanding adoption through strategic partnerships with educational and governmental bodies. In conclusion, DocVerify demonstrates that blockchain is not only a technological innovation but also a catalyst for reimagining the trust infrastructure of modern education, offering a future-proof solution to one of the most critical challenges in academic administration and digital identity management.

REFERENCES

1. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
2. Murthy, G. V., Kumar, C. P., & Kumar, V. V. (2017, December). Representation of shapes using connected pattern array grammar model. In *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 819-822). IEEE.
3. Krishna, K. V., Rao, M. V., & Murthy, G. V. (2017). Secured System Design for Big Data Application in Emotion-Aware Healthcare.
4. Rani, G. A., Krishna, V. R., & Murthy, G. V. (2017). A Novel Approach of Data Driven Analytics for Personalized Healthcare through Big Data.
5. Rao, M. V., Raju, K. S., Murthy, G. V., & Rani, B. K. (2020). Configure and Management of Internet of Things. *Data Engineering and Communication Technology*, 163.
6. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
7. Chithanuru, V., & Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: Challenges and future directions–A review. *Concurrency and Computation: Practice and Experience*, *35*(22), e7724.
8. Prashanth, J. S., & Nandury, S. V. (2015, June). Cluster-based rendezvous points selection for reducing tour length of mobile element in WSN. In *2015 IEEE International Advance Computing Conference (IACC)* (pp. 1230-1235). IEEE.
9. Kumar, K. A., Pabboju, S., & Desai, N. M. S. (2014). Advance text steganography algorithms: an

overview. *International Journal of Research and Applications*, *1*(1), 31-35.
10. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
11. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
12. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
13. Mahammad, F. S., Viswanatham, V. M., Tahseen, A., Devi, M. S., & Kumar, M. A. (2024, July). Key distribution scheme for preventing key reinstallation attack in wireless networks. In *AIP Conference Proceedings* (Vol. 3028, No. 1). AIP Publishing.
14. Lavanya, P. (2024). In-Cab Smart Guidance and support system for Dragline operator.
15. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
16. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7).
17. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, *255*.
18. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
19. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*, 179-184.
20. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
21. Raj, R. S., & Raju, G. P. (2014, December). An approach for optimization of resource management in Hadoop. In *International Conference on Computing and Communication Technologies* (pp. 1-5). IEEE.
22. Ramana, A. V., Bhoga, U., Dhulipalla, R. K., Kiran, A., Chary, B. D., & Reddy, P. C. S. (2023, June). Abnormal Behavior Prediction in Elderly Persons Using Deep Learning. In *2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3)* (pp. 1-5). IEEE.
23. Yakoob, S., Krishna Reddy, V., & Dastagiraiah, C. (2017). Multi User Authentication in Reliable Data Storage in Cloud. In *Computer Communication, Networking and Internet Security: Proceedings of IC3T 2016* (pp. 531-539). Springer Singapore.
24. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
25. Dastagiraiah, C., Krishna Reddy, V., & Pandurangarao, K. V. (2018). Dynamic load balancing environment in cloud computing based on VM ware off-loading. In *Data Engineering and Intelligent Computing: Proceedings of IC3T 2016* (pp. 483-492). Springer Singapore.
26. Swapna, N. (2017). „Analysis of Machine Learning Algorithms to Protect from Phishing in Web Data Mining“. *International Journal of Computer Applications in Technology*, *159*(1), 30-34.
27. Moparthi, N. R., Bhattacharyya, D., Balakrishna, G., & Prashanth, J. S. (2021). Paddy leaf disease detection using CNN.
28. Balakrishna, G., & Babu, C. S. (2013). Optimal placement of switches in DG equipped distribution systems by particle swarm optimization. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(12), 6234-6240.
29. Moparthi, N. R., Sagar, P. V., & Balakrishna, G. (2020, July). Usage for inside design by AR and VR technology. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-4). IEEE.
30. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
31. Amarnadh, V., & Moparthi, N. (2023). Data Science in Banking Sector: Comprehensive Review of Advanced Learning Methods for Credit Risk Assessment. *International Journal of Computing and Digital Systems*, *14*(1), 1-xx.
32. Amarnadh, V., & Rao, M. N. (2025). A Consensus Blockchain-Based Credit Risk Evaluation and Credit Data Storage Using Novel Deep Learning Approach. *Computational Economics*, 1-34.

33. Shailaja, K., & Anuradha, B. (2017). Improved face recognition using a modified PSO based self-weighted linear collaborative discriminant regression classification. *J. Eng. Appl. Sci*, *12*, 7234-7241.
34. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*.
35. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
36. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
37. Tejaswi, S., Sivaprashanth, J., Bala Krishna, G., Sridevi, M., & Rawat, S. S. (2023, December). Smart Dustbin Using IoT. In *International Conference on Advances in Computational Intelligence and Informatics* (pp. 257-265). Singapore: Springer Nature Singapore.
38. Moreb, M., Mohammed, T. A., & Bayat, O. (2020). A novel software engineering approach toward using machine learning for improving the efficiency of health systems. *IEEE Access*, *8*, 23169-23178.
39. Ravi, P., Haritha, D., & Niranjan, P. (2018). A Survey: Computing Iceberg Queries. *International Journal of Engineering & Technology*, *7*(2.7), 791-793.
40. Madar, B., Kumar, G. K., & Ramakrishna, C. (2017). Captcha breaking using segmentation and morphological operations. *International Journal of Computer Applications*, *166*(4), 34-38.
41. Rani, M. S., & Geetavani, B. (2017, May). Design and analysis for improving reliability and accuracy of big-data based peripheral control through IoT. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)* (pp. 749-753). IEEE.
42. Reddy, T., Prasad, T. S. D., Swetha, S., Nirmala, G., & Ram, P. (2018). A study on antiplatelets and anticoagulants utilisation in a tertiary care hospital. *International Journal of Pharmaceutical and Clinical Research*, *10*, 155-161.
43. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
44. AC, R., Chowdary Kakarla, P., Simha PJ, V., & Mohan, N. (2022). Implementation of Tiny Machine Learning Models on Arduino 33–BLE for Gesture and Speech Recognition.
45. Subrahmanyam, V., Sagar, M., Balram, G., Ramana, J. V., Tejaswi, S., & Mohammad, H. P. (2024, May). An Efficient Reliable Data Communication For Unmanned Air Vehicles (UAV) Enabled Industry Internet of Things (IIoT). In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-4). IEEE.
46. Nagaraj, P., Prasad, A. K., Narsimha, V. B., & Sujatha, B. (2022). Swine flu detection and location using machine learning techniques and GIS. *International Journal of Advanced Computer Science and Applications*, *13*(9).
47. Priyanka, J. H., & Parveen, N. (2024). DeepSkillNER: an automatic screening and ranking of resumes using hybrid deep learning and enhanced spectral clustering approach. *Multimedia Tools and Applications*, *83*(16), 47503-47530.
48. Sathish, S., Thangavel, K., & Boopathi, S. (2010). Performance analysis of DSR, AODV, FSR and ZRP routing protocols in MANET. *MES Journal of Technology and Management*, 57-61.
49. Siva Prasad, B. V. V., Mandapati, S., Kumar Ramasamy, L., Boddu, R., Reddy, P., & Suresh Kumar, B. (2023). Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 658-671.
50. Elechi, P., & Onu, K. E. (2022). Unmanned Aerial Vehicle Cellular Communication Operating in Non-terrestrial Networks. In *Unmanned Aerial Vehicle Cellular Communications* (pp. 225-251). Cham: Springer International Publishing.
51. Prasad, B. V. V. S., Mandapati, S., Haritha, B., & Begum, M. J. (2020, August). Enhanced Security for the authentication of Digital Signature from the key generated by the CSTRNG method. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1088-1093). IEEE.
52. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
53. Balaraju, J., Raj, M. G., & Murthy, C. S. (2019). Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. *Journal of Sustainable Mining*, *18*(4), 257-268.
54. Thirumoorthi, P., Deepika, S., & Yadaiah, N. (2014, March). Solar energy based dynamic sag compensator. In *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)* (pp. 1-6). IEEE.
55. Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain-Assisted Data

Transfer Mechanism in Healthcare-Based Cyber-Physical Systems. *Concurrency and Computation: Practice and Experience*, *37*(3), e8378.
56. Acharjee, P. B., Kumar, M., Krishna, G., Raminenei, K., Ibrahim, R. K., & Alazzam, M. B. (2023, May). Securing International Law Against Cyber Attacks through Blockchain Integration. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2676-2681). IEEE.
57. Ramineni, K., Reddy, L. K. K., Ramana, T. V., & Rajesh, V. (2023, July). Classification of Skin Cancer Using Integrated Methodology. In *International Conference on Data Science and Applications* (pp. 105-118). Singapore: Springer Nature Singapore.
58. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
59. Prasad, D. V. R., & Mohanji, Y. K. V. (2021). FACE RECOGNITION-BASED LECTURE ATTENDANCE SYSTEM: A SURVEY PAPER. *Elementary Education Online*, *20*(4), 1245-1245.
60. Dasu, V. R. P., & Gujjari, B. (2015). Technology-Enhanced Learning Through ICT Tools Using Aakash Tablet. In *Proceedings of the International Conference on Transformations in Engineering Education: ICTIEE 2014* (pp. 203-216). Springer India.
61. Reddy, A. M., Reddy, K. S., Jayaram, M., Venkata Maha Lakshmi, N., Aluvalu, R., Mahesh, T. R., ... & Stalin Alex, D. (2022). An efficient multilevel thresholding scheme for heart image segmentation using a hybrid generalized adversarial network. *Journal of Sensors*, *2022*(1), 4093658.
62. Srinivasa Reddy, K., Suneela, B., Inthiyaz, S., Hasane Ahammad, S., Kumar, G. N. S., & Mallikarjuna Reddy, A. (2019). Texture filtration module under stabilization via random forest optimization methodology. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 458-469.
63. Ramakrishna, C., Kumar, G. K., Reddy, A. M., & Ravi, P. (2018). A Survey on various IoT Attacks and its Countermeasures. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, *5*(4), 143-150.
64. Sirisha, G., & Reddy, A. M. (2018, September). Smart healthcare analysis and therapy for voice disorder using cloud and edge computing. In *2018 4th international conference on applied and theoretical computing and communication technology (iCATccT)* (pp. 103-106). IEEE.
65. Reddy, A. M., Yarlagadda, S., & Akkinen, H. (2021). An extensive analytical approach on human resources using random forest algorithm. *arXiv preprint arXiv:2105.07855*.
66. Kumar, G. N., Bhavanam, S. N., & Midasala, V. (2014). Image Hiding in a Video-based on DWT & LSB Algorithm. In *ICPVS Conference*.
67. Naveen Kumar, G. S., & Reddy, V. S. K. (2022). High performance algorithm for content-based video retrieval using multiple features. In *Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021* (pp. 637-646). Singapore: Springer Nature Singapore.
68. Reddy, P. S., Kumar, G. N., Ritish, B., SaiSwetha, C., & Abhilash, K. B. (2013). Intelligent parking space detection system based on image segmentation. *Int J Sci Res Dev*, *1*(6), 1310-1312.
69. Naveen Kumar, G. S., Reddy, V. S. K., & Kumar, S. S. (2018). High-performance video retrieval based on spatio-temporal features. *Microelectronics, Electromagnetics and Telecommunications*, 433-441.
70. Kumar, G. N., & Reddy, M. A. BWT & LSB algorithm based hiding an image into a video. *IJESAT*, 170-174.
71. Lopez, S., Sarada, V., Praveen, R. V. S., Pandey, A., Khuntia, M., & Haralayya, D. B. (2024). Artificial intelligence challenges and role for sustainable education in india: Problems and prospects. *Sandeep Lopez, Vani Sarada, RVS Praveen, Anita Pandey, Monalisa Khuntia, Bhadrappa Haralayya (2024) Artificial Intelligence Challenges and Role for Sustainable Education in India: Problems and Prospects. Library Progress International*, *44*(3), 18261-18271.
72. Yamuna, V., Praveen, R. V. S., Sathya, R., Dhivva, M., Lidiya, R., & Sowmiya, P. (2024, October). Integrating AI for Improved Brain Tumor Detection and Classification. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1603-1609). IEEE.
73. Kumar, N., Kurkute, S. L., Kalpana, V., Karuppannan, A., Praveen, R. V. S., & Mishra, S. (2024, August). Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach. In *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)* (pp. 1-6). IEEE.
74. Sharma, S., Vij, S., Praveen, R. V. S., Srinivasan, S., Yadav, D. K., & VS, R. K. (2024, October). Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1631-1636). IEEE.
75. Anuprathibha, T., Praveen, R. V. S., Sukumar, P., Suganthi, G., & Ravichandran, T. (2024, October). Enhancing Fake Review Detection: A Hierarchical Graph Attention Network Approach Using Text and Ratings.

In *2024 Global Conference on Communications and Information Technologies (GCCIT)* (pp. 1-5). IEEE.
76. Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1-6). IEEE.
77. Praveen, R. V. S., Hemavathi, U., Sathya, R., Siddiq, A. A., Sanjay, M. G., & Gowdish, S. (2024, October). AI Powered Plant Identification and Plant Disease Classification System. In *2024 4th International Conference on Sustainable Expert Systems (ICSES)* (pp. 1610-1616). IEEE.
78. Dhivya, R., Sagili, S. R., Praveen, R. V. S., VamsiLala, P. N. V., Sangeetha, A., & Suchithra, B. (2024, December). Predictive Modelling of Osteoporosis using Machine Learning Algorithms. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 997-1002). IEEE.
79. Kemmannu, P. K., Praveen, R. V. S., Saravanan, B., Amshavalli, M., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)* (pp. 724-730). IEEE.
80. Praveen, R. V. S. (2024). *Data Engineering for Modern Applications.* Addition Publishing House.