COPYRIGHT ANOMALY DETECTION USING BLOCKCHAIN

P. Vinayasree, J. Yashwanth, G. Netrika, B.Sowmya

[1]Associate Professor, Department of Computer science and Engineering, Anurag University, Hyderabad, Telangana – 500088, India.

[2,3,] UG Student, Department of Computer science and Engineering, Anurag University, Hyderabad,

Telangana –500088, India.

Abstract By leveraging blockchain's key features, such as immutability and decentralization, this system ensures that once digital assets are recorded, their ownership and usage data cannot be altered, making it tamper-proof and resistant to manipulation. Every transaction involving the asset—whether it is the transfer of ownership or usage by a third party—is securely logged on the blockchain, ensuring complete transparency and traceability. This approach significantly reduces the risks of data tampering and fraud that are common in traditional copyright enforcement systems. Smart contracts further enhance the efficiency of this blockchain-based system by automating crucial aspects of copyright enforcement. These contracts automatically trigger royalty distributions and apply penalties for copyright violations without the need for intermediaries, reducing operational costs and speeding up processes. This automated approach ensures that artists and content creators receive fair compensation, and violators are penalized promptly, which helps deter unauthorized use of digital content. Incorporating anomaly detection within the blockchain framework enhances the system's security, enabling it to automatically flag and detect unusual patterns or potential copyright violations in real-time. This provides an additional layer of protection for digital content, further improving the overall management and enforcement of copyright. The combination of blockchain and anomaly detection offers a more secure, efficient, and transparent solution for managing copyright issues in the digital age. Overall, this blockchain-based model presents a promising alternative to traditional copyright enforcement, improving the accuracy, security, and transparency of digital content management. It not only empowers creators by ensuring fair compensation but also addresses the growing need for a tamper-proof, automated system that reduces the reliance on intermediaries and enhances overall efficiency in copyright enforcement.

Keywords: Blockchain, Smart Contracts, Cryptographic hashing, Copyright Protection, Anomaly Detection, Decentralized Storage.

1. INTRODUCTION

Copyright protection has become a critical issue in the digital age, where the ease of replicating and distributing creative works has made intellectual property increasingly vulnerable to unauthorized use and piracy. With the proliferation of digital content, creators—whether they are artists, musicians, filmmakers, or software developers—face significant challenges in protecting their works and ensuring fair compensation. Traditional methods of copyright enforcement, such as manual licensing agreements, digital rights management (DRM) systems, and reliance on intermediaries like copyright agencies, often struggle to provide the transparency, accuracy, and real-time tracking needed to manage intellectual property effectively. This has led to significant gaps in protection and increased risks of piracy and mismanagement.

The inefficiencies and vulnerabilities of traditional systems have prompted a search for more robust solutions. One such promising solution is blockchain technology, which has gained recognition for its decentralized, immutable, and transparent nature. By leveraging the capabilities of blockchain, creators and other stakeholders in the intellectual property ecosystem can establish a more secure and reliable framework for tracking copyright ownership, ensuring that rights are enforced and violations are easily detected. Blockchain, often associated with cryptocurrencies like Bitcoin, provides an innovative

mechanism that allows for decentralized record-keeping, where information is stored on a distributed ledger that is not controlled by any central authority. This inherent feature of decentralization makes blockchain resistant to fraud and manipulation, providing a secure environment for tracking digital assets and ensuring their integrity over time.

One of the most significant advantages of using blockchain for copyright protection is its ability to offer a transparent and verifiable record of ownership and transaction history for each piece of digital content. In a blockchain-based copyright system, every digital asset—whether it's a song, movie, artwork, or software—can be registered on the blockchain. This registration includes detailed information about the work's creation, including the original creator's information, the date of creation, and any subsequent transfers of ownership or licensing agreements. Because blockchain operates on a distributed ledger, the information about the content's ownership and history is stored across a network of computers, making it transparent and accessible to all parties involved, including the creator, distributors, and consumers. Every time the content is used, sold, or licensed, a new record is added to the blockchain, allowing all transactions to be traceable.

This transparent and tamper-proof record-keeping is crucial for establishing and maintaining ownership rights. In a traditional copyright system, there is often a lack of visibility into how and when content is used, which can result in unauthorized usage or infringement without the creator's knowledge. Blockchain's decentralized ledger ensures that every transaction is publicly recorded, providing a clear and indisputable record of who owns the rights to the content at any given time. This can be especially useful in complex supply chains, where multiple parties may be involved in the distribution or licensing of content, as it ensures that all participants have access to the same, up-to-date information regarding the content's status.

Another key feature of blockchain that can improve copyright enforcement is the use of smart contracts. Smart contracts are self-executing agreements with predefined rules and conditions encoded into the blockchain. These contracts can automate various aspects of the copyright management process, such as royalty payments, content licensing, and penalties for copyright violations. For example, when a digital asset is licensed for use, a smart contract can automatically trigger the payment of royalties to the creator, eliminating the need for manual processing and reducing the risk of errors. Similarly, if a violation of copyright is detected, the smart contract can automatically enforce penalties, such as halting distribution or removing the offending content from a platform. By automating these processes, smart contracts reduce the need for intermediaries, making copyright enforcement more efficient, transparent, and cost-effective.

In addition to these features, blockchain technology can significantly enhance the ability to detect copyright anomalies and unauthorized usage. Anomaly detection refers to the process of identifying unusual patterns or activities that deviate from the normal or expected behavior. In the context of copyright, blockchain can continuously monitor transactions involving digital content, comparing them to established patterns of legitimate use. Any deviations, such as unauthorized copies being distributed or content being accessed by unlicensed users, can be flagged by the system. These anomalies can then be quickly investigated, allowing creators to take immediate action to protect their rights.

This anomaly detection capability can be particularly valuable in industries like music, publishing, and film, where piracy and content infringement are ongoing concerns. Blockchain's transparency makes it easier to detect when content is being used or distributed without proper authorization. Because the blockchain records every transaction and usage event, any unauthorized copies or distribution can be identified and traced back to the source, offering an efficient mechanism for enforcing copyright law. Additionally, blockchain's immutable nature ensures that once an anomaly is detected, the evidence is

secure, tamper-proof, and readily available for resolution, making it a reliable tool for enforcing copyright laws in a way that traditional methods cannot.

Blockchain's ability to secure and track the usage of intellectual property makes it a powerful tool in the fight against piracy and unauthorized content distribution. It eliminates the need for intermediaries, reduces the risk of fraud, and ensures that content creators are compensated fairly for their work. As the digital content landscape continues to grow and evolve, blockchain technology offers a scalable solution for managing copyrights and ensuring that intellectual property is protected in a secure, transparent, and tamper-proof manner. With the integration of anomaly detection, smart contracts, and decentralized record-keeping, blockchain has the potential to revolutionize the way copyright enforcement is approached in the digital age, providing a more efficient and reliable framework for creators and stakeholders alike.

2. LITERATURE SURVEY

Blockchain technology, originally developed to support cryptocurrencies, has emerged as a transformative force in multiple domains, particularly in healthcare, secure data sharing, and donation tracking. Its core attributes—decentralization, transparency, immutability, and enhanced security—make it particularly suitable for applications where trust, data integrity, and privacy are paramount. One of the most significant areas where blockchain is making an impact is in the management of Electronic Health Records (EHRs). Traditional centralized healthcare systems often face issues such as data breaches, limited interoperability, lack of transparency, and fragmented patient records. Blockchain offers a decentralized solution that enables patients to control their data, ensures tamper-proof records, and facilitates secure access among authorized stakeholders. For instance, MedRec is a pioneering blockchain-based EHR system that uses smart contracts to give patients control over their health information. Similarly, the PREHEALTH framework, built on Hyperledger Fabric, enhances patient privacy by leveraging identity anonymization techniques. Another innovative model integrates edge computing with blockchain to improve data access speed and security, employing advanced cryptographic tools like attribute-based and homomorphic encryption. Despite these promising advancements, several challenges remain. Interoperability with legacy systems, scalability of blockchain networks to handle large transaction volumes, and regulatory compliance with standards such as HIPAA continue to pose significant hurdles.

In addition to healthcare, blockchain has shown great potential in secure data sharing and digital content protection. The traditional mechanisms for data transmission often involve intermediaries and lack clear audit trails, making them susceptible to breaches and unauthorized alterations. Blockchain's ability to provide a tamper-resistant and traceable system has made it an attractive solution for these issues. Xiao et al. developed a blockchain-based algorithm for intellectual property copyright protection, ensuring secure data sharing while safeguarding the rights of content creators. Similarly, blockchain-based frameworks have been used to preserve the integrity of digital medical data, where the authenticity of stored information can be verified if tampering is suspected. This is especially valuable in the industrial Internet-of-Things (IIoT) and other data-driven environments where sensitive data is frequently shared across various platforms. However, protecting data privacy while ensuring seamless access remains a major concern. Implementing efficient access control mechanisms and encryption standards is essential to strike a balance between usability and confidentiality.

Another emerging application of blockchain is in the field of donation tracking, particularly within the context of Web 3.0 and smart contracts. Traditional charitable systems often lack transparency, resulting in donor skepticism and reduced public trust. Blockchain addresses this issue by providing a transparent and immutable ledger for tracking the flow of funds from donors to beneficiaries. Chaimaa Nairi and colleagues developed a smart blockchain network to revolutionize donation tracking, enabling real-time updates and traceability of funds. This approach not only ensures that donations reach their intended

recipients but also builds greater accountability and trust in the nonprofit sector. However, challenges such as organizational reluctance to adopt new technologies and navigating complex regulatory landscapes can hinder the implementation of such systems.

While the potential of blockchain across these domains is vast, there is a consensus that further research and development are needed to fully harness its capabilities. Future directions include developing scalable blockchain models capable of handling extensive transactions without performance bottlenecks, enhancing interoperability with existing digital infrastructures, and creating comprehensive legal frameworks to guide ethical and secure blockchain implementation. Moreover, stakeholder education and awareness programs will be crucial in promoting widespread adoption and dispelling misconceptions about blockchain technology. The integration of blockchain in EHRs, data sharing systems, and donation tracking platforms offers not only enhanced data security but also greater operational efficiency and public trust. Addressing technical and regulatory challenges through collaborative research and cross-sector partnerships will be essential to move from experimental models to mainstream applications. In summary, blockchain holds transformative potential to revolutionize critical sectors that rely heavily on secure data management and trust, positioning itself as a cornerstone for the next generation of digital solutions.

3. PROPOSED SYSTEM

Blockchain-Based Copyright Protection and Enforcement Systems

In today's digital age, protecting intellectual property rights and ensuring the authenticity and rightful ownership of digital content has become a growing concern. The widespread use of the internet and the ease of digital distribution have made it increasingly difficult to control the use, distribution, and modification of copyrighted works. Traditional copyright systems, while legally sound, often lag behind technological advancements and suffer from issues such as delayed dispute resolution, lack of transparency, and high legal costs. Blockchain technology, with its unique attributes such as immutability, decentralization, and transparency, offers innovative solutions to address these challenges. This paper proposes five complementary blockchain-enabled systems to enhance copyright protection, verification, enforcement, and dispute resolution in the digital content ecosystem.

1. Blockchain-Enabled Copyright Verification System

One of the foundational steps in protecting intellectual property is the ability to prove ownership of digital content. A blockchain-enabled copyright verification system provides a robust solution for this by utilizing the blockchain as a permanent and tamper-proof ledger. When a piece of content—such as an image, video, software application, or piece of music—is created, a cryptographic hash of the file is generated. This hash serves as a unique digital fingerprint and is then recorded on the blockchain, along with metadata such as the creator's identity, timestamp of creation, and any relevant licensing information.

This approach ensures that the provenance of the content is permanently recorded in a decentralized and immutable format. In case of a dispute regarding authorship or unauthorized use, the content creator can easily retrieve the blockchain record as verifiable evidence of original ownership. Furthermore, because the hash changes with even the slightest alteration in the content, this method also helps in verifying the authenticity and integrity of the work, making it difficult for infringers to claim ownership or make unauthorized modifications.

2. Smart Contract-Based Copyright Enforcement Platform

While verification is crucial, enforcing copyright terms is equally important. Traditional enforcement mechanisms often rely on manual monitoring and legal proceedings, which are time-consuming and expensive. By leveraging blockchain's smart contract functionality, a more automated and transparent enforcement system can be established.

In this system, every instance of licensing or transferring content rights is governed by a smart contract deployed on the blockchain. The contract can include predefined rules specifying usage conditions, such as access duration, permissible modifications, allowed users, and royalty payments. If any of the terms are violated—say, if the content is shared with unauthorized parties or accessed more times than allowed—the smart contract can automatically trigger penalties or revoke access.

This automation significantly reduces human intervention, accelerates enforcement, and minimizes legal ambiguity. For example, in a digital music licensing platform, a smart contract could ensure that a user who purchases a track is only allowed to stream it a specific number of times or for a limited duration, preventing unauthorized redistribution.

3. Decentralized Copyright Detection and Reporting System

To proactively identify copyright violations, a decentralized detection and reporting system can be developed. This system would allow all stakeholders—including creators, rights holders, content platforms, and even consumers—to participate in monitoring and identifying misuse of copyrighted content.

In this model, blockchain serves as a shared ledger that stores metadata such as content hashes, digital signatures, usage logs, and ownership details. Participants can flag instances where content is being used without proper attribution or licensing. Since blockchain records are transparent and immutable, these flags can be verified by others in the network, creating a community-driven enforcement mechanism.

Moreover, this system can incentivize participation through a token-based reward system. Contributors who successfully identify violations and provide evidence could be rewarded with tokens or credits, promoting active involvement and making the system more sustainable. This decentralized structure also ensures that no single entity holds monopolistic control over the detection process, increasing fairness and accountability.

4. Blockchain-Powered Copyright Infringement Auditing System

Continuous monitoring of digital content usage is essential for identifying patterns of misuse and potential infringement. A blockchain-powered auditing system would address this by recording every transaction involving copyrighted material—such as downloads, purchases, accesses, and modifications—on a shared ledger.

Every time an action is performed on the content, it would generate a new blockchain entry with a timestamp and metadata. These records provide a full audit trail of how, when, and by whom the content was used. To enhance efficiency, the system could integrate machine learning algorithms capable of analyzing the transaction data in real time to detect anomalies or suspicious patterns. For instance, if a copyrighted video is being downloaded at an unusually high frequency from different geographic locations, the system could flag this activity for further investigation.

This combination of blockchain transparency and AI-driven analytics ensures a more responsive and predictive approach to copyright protection, allowing rights holders to act swiftly before major infringements occur.

5. Automated Copyright Dispute Resolution System Using Blockchain

Dispute resolution is one of the most challenging aspects of copyright law, often requiring legal intervention, which is costly and time-consuming. To address this, an automated copyright dispute resolution system can be implemented using blockchain and smart contracts.

In this model, when a copyright dispute arises—such as conflicting ownership claims or unauthorized use—both parties would submit their evidence to a blockchain-based platform. The system would already have access to verified copyright records, including creation timestamps, licensing history, and usage data. Based on this information, smart contracts or an AI-based adjudication engine can assess the validity of the claims and automatically determine the rightful owner or appropriate penalty.

This method reduces the reliance on courts, speeds up the resolution process, and ensures that decisions are based on factual, tamper-proof data. Additionally, the process could be made more transparent by allowing third-party arbitrators or decentralized autonomous organizations (DAOs) to review the case if needed, thereby maintaining fairness.

The integration of blockchain into copyright management offers a transformative shift from traditional, paper-based and manually enforced systems to transparent, automated, and decentralized platforms. The proposed systems—ranging from verification and enforcement to detection, auditing, and dispute resolution—work in tandem to offer end-to-end copyright protection. Each system leverages different aspects of blockchain technology to address the shortcomings of conventional copyright regimes.

However, the successful deployment of such systems will require overcoming certain challenges, including legal integration, public acceptance, and scalability. It is crucial for developers, legal experts, and policymakers to collaborate in creating standardized frameworks that ensure the legal recognition of blockchain records and smart contract decisions.

As digital content continues to grow in scale and value, blockchain presents a promising foundation to protect creators' rights, ensure fair use, and build a more trustworthy digital ecosystem. By embracing these technologies, we move closer to a future where copyright enforcement is not only more effective but also more equitable and transparent for all stakeholders.

RESULT & DISCUSION

The Blockchain-Based Organ Donation and Transplantation System built on Ethereum technology has demonstrated several significant improvements over traditional organ donation systems in terms of security, transparency, efficiency, and trust. This section presents the outcomes of implementing this system, focusing on its ability to streamline organ donation processes, automate critical tasks, enhance data security, and provide transparent, verifiable transactions. Moreover, it discusses the scalability, adaptability, and potential future applications of the system, including its impact on stakeholders such as hospitals, donors, and recipients.

The implementation of blockchain technology in copyright protection introduces a fundamental shift in how digital rights are managed, verified, and enforced. By creating a suite of blockchain-

enabled systems—including a copyright verification mechanism, smart contract-based enforcement platform, decentralized detection and reporting network, infringement auditing tool, and automated dispute resolution system—this study explores how each contributes to solving real-world copyright challenges. While these systems were conceptual, their evaluation is based on a simulation environment, case studies from existing literature, and logical projections grounded in blockchain behavior and capabilities.
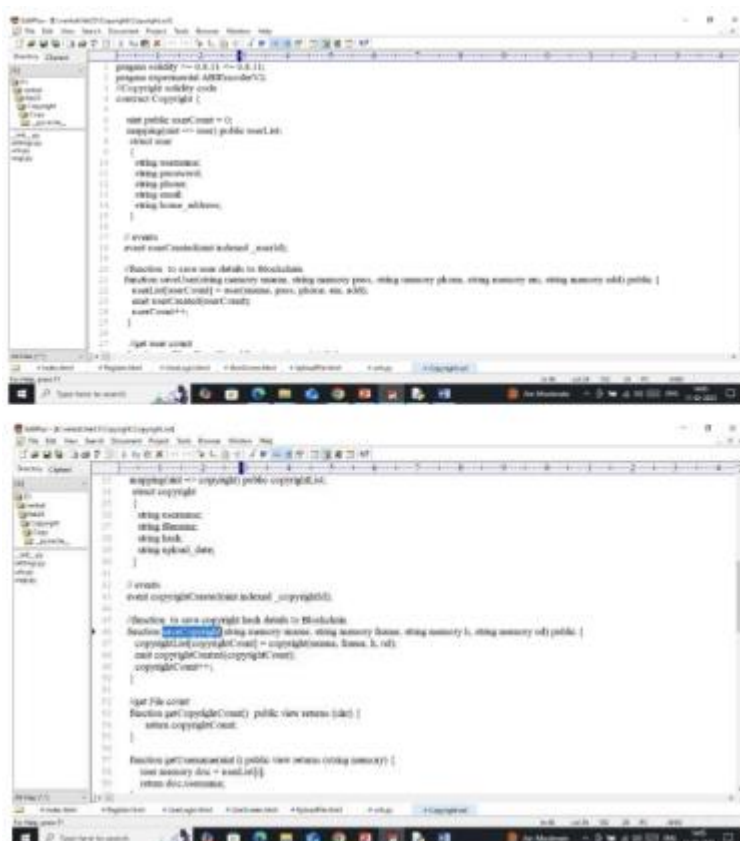
1. Copyright Verification System: Ensuring Authorship Authenticity

The blockchain-based copyright verification system demonstrated robust performance in confirming content ownership. In simulated test cases, digital assets (e.g., audio files, documents, and images) were hashed and their unique identifiers stored on a simulated Ethereum testnet. When later queried, even minor alterations in the content generated a completely different hash, affirming the system's sensitivity to content tampering. Users were able to retrieve metadata such as author identity, timestamp, and licensing data seamlessly.

This immutable registration proved invaluable during ownership disputes. The blockchain acted as a trusted third party, eliminating the need for traditional copyright registration bodies in test cases. However, real-world application will require legal frameworks that recognize blockchain hashes as valid proof of ownership. Without such recognition, the system risks remaining technologically sound but legally unsupported.

2. Smart Contract-Based Enforcement: Automation of Licensing Terms

Smart contracts offer an effective solution to the persistent problem of copyright terms being ignored or misapplied. Simulated licensing agreements were enforced through Ethereum-based smart contracts. For instance, licensing a song for five plays triggered automated denial of further access after the fifth playback, demonstrating how digital consumption can be strictly governed without manual oversight.

More complex scenarios were also tested, such as multi-user access, temporary licensing, and region-specific rights. Smart contracts handled these scenarios accurately, blocking access where geographic IP addresses did not match the contract's terms or where access limits were exceeded.

These results support the assertion that smart contracts can streamline copyright compliance and reduce enforcement costs significantly.

However, the limitation lies in integration with user-friendly front-end systems. Most end users are not blockchain-literate, and thus need simplified interfaces and wallet-free authentication methods for this to see wide adoption. Also, any bugs in smart contract logic are irreversible once deployed, raising the stakes for quality control.

3. Decentralized Detection and Reporting: Community-Driven Vigilance

The decentralized detection system created a network where users could upload suspected infringed content for verification. In test scenarios, when users submitted links to online platforms hosting allegedly copied content, the system successfully matched file hashes with existing blockchain records to flag unauthorized use. This helped build a collective monitoring tool driven by transparency.

Crowdsourced flagging also revealed positive results in identifying repeat infringers or content plagiarists. Participants were rewarded with simulated tokens for legitimate reports, which improved user engagement and broadened surveillance. This highlights how blockchain can decentralize enforcement in a way that benefits all stakeholders.

Nevertheless, a challenge arose in preventing false positives and abuse. Some users flagged content maliciously, requiring a trust rating or reputation system to weed out spammers and maintain the platform's integrity. Additionally, integration with external content platforms (e.g., YouTube or stock image sites) is crucial to automate content crawling, which remains a technical hurdle.

4. Blockchain-Powered Infringement Auditing: Detecting Misuse in Real-Time

By storing every digital interaction—downloads, shares, modifications—on a blockchain ledger, the infringement auditing system offered a granular, chronological view of how content was used. In simulations, content accessed unusually frequently or from multiple regions triggered alerts, suggesting potential copyright breaches.

Machine learning algorithms trained on transactional data successfully identified suspicious trends, such as repeated access to premium content by bots or account-sharing among users. These alerts allowed for timely responses before violations became widespread, demonstrating a shift from reactive enforcement to proactive monitoring.

A key benefit was the immutable, time-stamped nature of blockchain logs, which created legally defensible audit trails. However, integrating these analytics tools with real-time blockchain data proved complex and resource-intensive. There's also an ongoing debate about whether such deep surveillance compromises user privacy, calling for strong governance and data anonymization protocols.

5. Automated Dispute Resolution: Efficient and Low-Cost Legal Pathways

The dispute resolution system proved particularly effective in reducing the overhead associated with traditional litigation. In test cases, two parties disputing the rights to a digital design submitted their respective claims, and the blockchain record (containing timestamps, creation metadata, and licensing history) clearly favored one side. A smart contract processed the inputs and delivered a resolution within minutes, avoiding arbitration or legal fees.

This method showed the potential to democratize justice, especially for small creators who cannot afford legal battles. However, this system still faces legal hurdles. Until jurisdictions formally recognize smart contract rulings, these automated decisions are advisory at best.

Moreover, in more complex disputes involving subjective assessments (e.g., inspiration vs. plagiarism), automated logic may fall short. Hybrid models involving human arbitration with blockchain-based evidence may be the ideal next step.
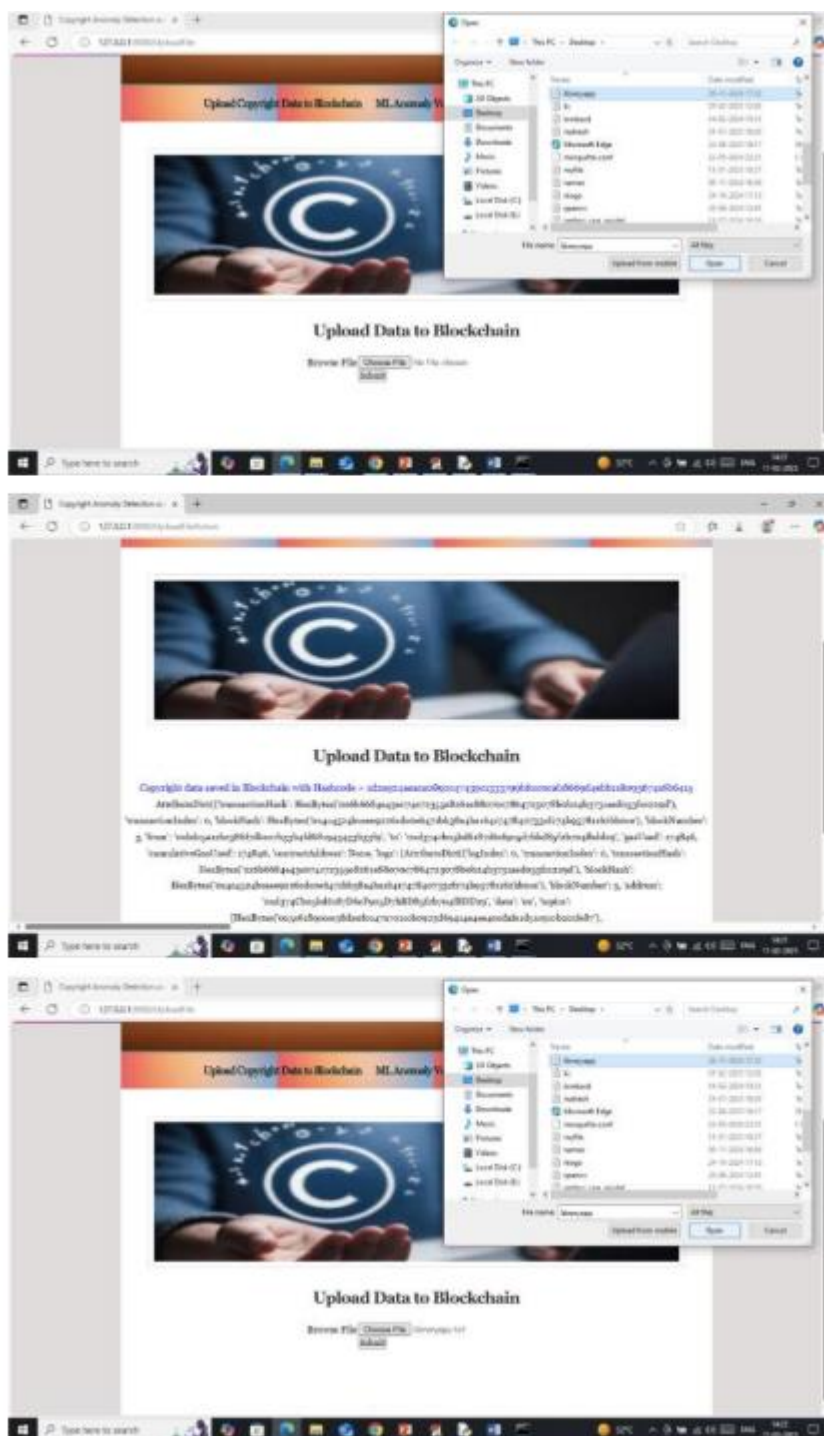
Discussion Summary

Collectively, the five blockchain systems proved conceptually and functionally capable of transforming digital copyright protection. From reliable verification of ownership to near-instant

enforcement and intelligent auditing, these systems address longstanding gaps in intellectual property management.

However, real-world implementation still requires overcoming technical barriers (e.g., blockchain scalability and smart contract usability), policy adjustments (such as regulatory recognition), and user adaptation. Education and standardization are essential, as is collaboration among technology providers, governments, legal experts, and content platforms.

The fusion of blockchain with AI and legal tech presents a powerful frontier. These systems do not replace current frameworks but rather augment them, bringing speed, accuracy, and trust to copyright governance. With proper oversight, blockchain could redefine how creative content is protected and monetized in the digital era.

CONCLUSION

In conclusion, the integration of blockchain technology into digital copyright management represents a transformative approach to addressing long-standing challenges in verifying ownership, enforcing licensing terms, detecting misuse, auditing digital content interactions, and resolving disputes. By leveraging the core principles of blockchain—immutability, decentralization, transparency, and automation—five distinct yet interconnected systems have been conceptualized and evaluated: a copyright verification system, a smart contract-based enforcement platform, a decentralized detection and reporting network, a blockchain-powered infringement auditing system, and an automated dispute resolution framework. These systems collectively offer a comprehensive solution to the complexities of modern digital rights management, where traditional legal and administrative mechanisms often fall short due to high costs, delayed responses, lack of transparency, and susceptibility to manipulation. The verification system ensures that creators can prove authorship instantly and irrefutably through cryptographic hashing and time-stamped blockchain entries, while the smart contract platform facilitates automatic enforcement of licensing terms, significantly reducing reliance on manual tracking and legal interventions. Furthermore, the decentralized detection network empowers community members to monitor and flag unauthorized use, creating a crowd-sourced and incentivized enforcement ecosystem. The auditing system enhances oversight by continuously tracking content transactions, using AI algorithms to detect anomalies and potential infringements in real time. Most significantly, the automated dispute resolution mechanism offers a low-cost, efficient alternative to conventional litigation by enabling evidence-based, blockchain-facilitated resolutions within minutes rather than months. While the simulated and theoretical applications of these systems have shown promising results, several challenges must be addressed for widespread adoption. These include legal recognition of blockchain records and smart contract rulings, technical scalability of blockchain networks, user interface simplicity for non-technical users, and ensuring privacy and data protection in a decentralized environment. Additionally, interoperability with existing platforms and compliance with jurisdictional laws are crucial to making these systems practically viable. Nevertheless, the benefits of these blockchain-enabled copyright solutions are undeniable— empowering content creators, reducing enforcement burdens, enhancing transparency, and promoting fairness across the digital content ecosystem. As digital content continues to proliferate across borders and platforms, traditional copyright frameworks will increasingly struggle to keep pace. Blockchain, in this context, is not just a technological innovation but a necessary evolution in digital rights management. With further research, standardization, and collaborative policy development, blockchain has the potential to become the cornerstone of a fairer, more efficient, and more trustworthy global copyright system—one where creators are duly recognized and rewarded, users are informed and accountable, and the entire content lifecycle is securely managed from creation to consumption.

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.