

# A Hybrid Blockchain–Al Architecture for Secure and Transparent Decentralized Crowdfunding

B. S. Lakshmi<sup>1,2</sup> and K. S. Rekha<sup>1,3</sup>

<sup>1</sup>The National Institute of Engineering, Mysuru, affiliated to Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>Department of Computer Science, Vidyavardhaka College of Engineering, Mysuru,

affiliated to Visvesvaraya Technological University, Belagavi, India

<sup>3</sup>Department of Computer Science and Engineering, JSS Science and Technology, Mysuru, India

(Received 28 May 2025; Revised 23 September 2025; Accepted 17 October 2025; Published online 10 November 2025)

Abstract: Crowdfunding websites tend to have centralized escrow infrastructure, which can create concerns over the lack of transparency, security threats, and fraud vulnerability. The proposed system, a hybrid blockchain–AI architecture, combines Ethereum-based smart contracts and machine learning-based fraud detection to result in a decentralized and transparent crowdfunding space. The blockchain layer ensures accountability with controlled release of funds based on milestones, limiting the tendency to spend funds more due to the cryptocurrency nature with the AI module detecting fraudulent activity based on analysis of textual, transactional, temporal, and reputation data. Experimentation proves that the proposed system promotes higher trust, reduces transaction cost, and signifies a robust fraud detection model compared to conventional crowdfunding models. The results suggest creating a combination of the immutability of blockchains with the analytical power of AI as a potential route to safer and more effective decentralized finance apps.

Keywords: blockchain technology; crowdfunding; machine learning; milestone-based fund management; smart contracts

#### I. INTRODUCTION

Crowdfunding has been a revolutionary form of finance that allowed creators and start-up groups to raise money directly rather than having to organize themselves through conventional mediums. This democratic system of funding has boosted the distribution of early-stage finance, especially those ventures whose ancillary is not collaterally supported or traditional. The world market of crowdfunding has jumped to 14.2 billion in 2021 and is expected to experience a 16.7% Compound Annual Growth Rate to reach a total of 28.8 billion in 2028 [1]. Although this growth has been made possible by centralized crowdfunding platforms, which host campaigns and charge a 5–10% commission to handle transactions [2], this type of structure has created limitations that limit the potential of the ecosystem.

This paper investigates the combination of security and decentralized finance with respect to crowdfunding through the intertwining of blockchain and AI. Blockchain provides transparent, permanent transactions and fund control based on smart contracts, whereas AI can improve security based on pattern recognition and fraud identification. This work develops a unified architecture specifically suited to a crowdfunding application unlike previous researches which had the technologies independently. This hybrid system is more secure, transparent, and cost-effective compared to classical platforms. In spite of their booming development, there are still some decisive obstacles related to crowdfunding. Traditional platforms can be characterized by centralized control in project approval, management of funds,

and resolution of disputes, and risks can be specified as a non-transparency level and single points of failure. There is the issue of trust, where only 86 % of the projects are delivered successfully and about 3–5 % involve deliberate fraud. Furthermore, it is discovered that a large number of prospective investors do not participate in it because they are afraid that the money would be misused and there should be no accountability [3]. Such problems affect the credibility of the platform and slow down the growth to the market.

The manual approach to fraud detection in crowdfunding is inadequate. Machine learning is more accurate, but it is infeasible to use in decentralized systems due to privacy and computational requirements [4,5]. In addition, the all-or-nothing funding system is highly risky, since creators get all the money whether the project succeeds or not. The lack of a milestone-based fund release, cross-border regulatory issues, and the absence of transparent verification mechanisms are additional obstacles to trust and innovation [6].

The immutability, transparency, and smart contract properties of blockchain have contributed to its popularity in crowdfunding. Its application was illustrated by Abdali *et al.* [7] in strengthening e-government security by means of mobile/web integration and validation protocols. Tripathi and Al Shahri [8] observed that distributed ledgers foster trust through cryptographic checking, but the complexity of technology is an impediment. Kavithamani *et al.* [9] demonstrated that Ethereum-based crowdfunding betters fund traceability by lowering intermediary expenses by up to 70%, yet scale issues remain. In the context of decentralized resource management, Kanike [10] expressed similar concerns. According to Yuvarasu *et al.* [11], wireless sensor verification was 93.8% accurate, which could be applied to releasing tokens. There are also regulatory issues, where Cruz Angeles *et al.* [12] emphasize the

importance of balanced policies that can help to promote innovation and protect the user.

Fattoh *et al.* [13] suggested that a transformer-based sentiment model that uses universal sentence encoders can identify misleading content with 91.2% accuracy, albeit at high computational cost. Karna *et al.* [14] proposed the Bidirectional Long Short-Term Memory with Naïve Bayes integration model, which detects fraud earlier by 27% than traditional models. Multimodal methods are also promising: Priscila and Jayanthiladevi [15] achieved 94.3% accuracy with 22 fewer false positives in hybrid Deep Learning (DL), and Priscila *et al.* [16] discovered that KNN was effective for complex classification with low overhead, which can be useful in blockchain systems. Sharma and Tripathi [17] used intuitionistic fuzzy similarity to estimate financial risks in trust modeling, and Sharma and Sharma [18] detected trends and abnormalities to early detect fraud.

There is a lack of research on blockchain and AI in crowd-funding. Senapati and Rawal [19] introduced a split-protocol DL model, which enhanced prediction accuracy but minimized overhead by selectively executing on-chain. Arumugam *et al.* [20,21] used big data to increase fund allocation transparency through digital representation. A study by Sommro *et al.* [22] also combined AI and smart contracts, minimizing the communication errors by 47%. Regin *et al.* [23] demonstrated that ensemble-based supervised learning enhances decision-making in complex systems. Naeem *et al.* [24] developed a hybrid control system of autonomous cars, providing information on how to balance automation and human control in decentralized financing.

# II. METHODOLOGY

This part describes the architecture of the hybrid blockchain–AI crowdfunding system (Fig. 1), which is developed based on four main components: blockchain layer, artificial intelligence module, decentralized storage, and user interface. The blockchain layer provides safe, irreversible transactions with conditional release of funds through smart contracts. Fraud detection is also possible through the AI module, which monitors campaign activity in near real time. Storage is decentralized, which maintains accessibility and data integrity of project media and records. The user interface is

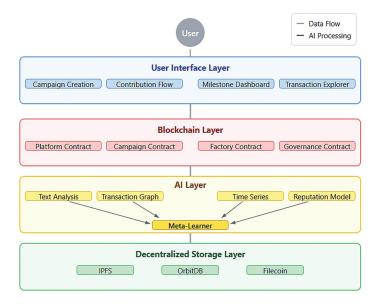


Fig. 1. System architecture of the hybrid blockchain-AI crowdfunding.

user-friendly with easy accessibility to essential functions. All elements communicate by encrypted Application Programming Interfaces, and cryptographic protocols ensure integrity and authenticity.

# A. BLOCKCHAIN LAYER

The system is based on the Ethereum blockchain and relies on a modular pool of smart contracts to manage campaigns, distribute funds, and govern it, securing transparent and automated operations. The architecture comprises (i) a Platform Contract regarding service fees and registration policies, (ii) a Campaign Factory Contract regarding automatic campaign creation, (iii) a Campaign Contract regarding escrow, milestone monitoring, and stakeholder services, and (iv) a Governance Contract allowing a decentralized decision-making process through voting and dispute resolution.

One of the main advances of this architecture is the milestone-based fund release mechanism. In contrast to conventional models that discharge funds after objective attainment, the distribution is done in authenticated growth phases. Money is held in escrow in the Campaign Contract and is only released once milestones are approved by the backers or moderators. This will increase accountability and minimize chances of fund misappropriation or project abandonment. The pseudocode is presented in Fig. 2.

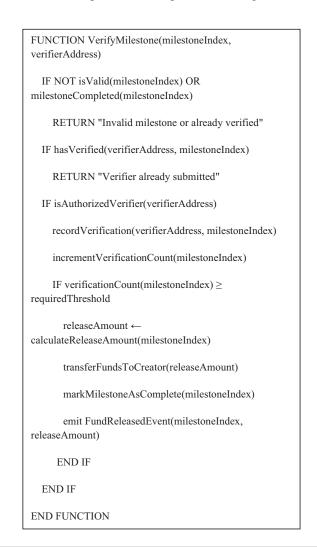


Fig. 2. Milestone verification and conditional fund release.

The conditional release method allows money to be issued to the project only when validation occurs by both sides, and it helps in ensuring that there is a minimum probability of fraud and there is correspondence of expenses with respect to the progress of the project. The system is constructed on the basis of sound verification mechanisms that have been modeled on the principles of trust as postulated by Sharma and Tripathi [17].

#### **B. AI LAYER**

The AI layer can use a multimodel ensemble framework to assess real-time fraud and risk, based on methods by Fattoh *et al.* [13] and Silvia Priscila and Jayanthiladevi [15], to increase platform security. The Text Analysis Model is a transformer-based Natural Language Processing that finds deceptive language in descriptions and comments. Based on Graph Neural Networks, the Transaction Graph Model discovers suspicious relationships among contributors. Based on LSTM, the Time Series Model identifies abnormal financial activities, such as bursts or lack of activity. The Creator Reputation Model provides an evaluation of historical and behavioral metrics in gradient-boosted trees by evaluating the reputation of campaign creators. A meta-learner combining the outputs of these models will adaptively weight each prediction according to the previous accuracy to enhance the accuracy of the final fraud risk score, as well as improve the interpretability of the score.

The fraud detection system can work on three temporal zones to guarantee the integrity of platforms and active risk prevention. The first, pre-launch analysis, analyzes campaigns prior to publication to address those with high risks at an early stage. The second, continuous monitoring, performs the adjustment of risk scores in real time, in accordance with constant user behavior. Milestone verification is the third one, as it evaluates legitimacy every time the release of funds occurs. Such a multilayered system is more responsive and reduces the occurrence of false positives, which fits the predictive system suggested by Senapati and Rawal [19]. The platform will utilize a hybrid decentralized data storage stability to allow safe and reliable data management. InterPlanetary File System uses content-addressable hashes to provide data integrity of the stored iconic material like images, videos, and documents. OrbitDB includes real-time responses, comments, and updates by users, including frequent changes. Filecoin offers permanent storage of finalized campaign data so that it can be archived and cause compliance with regulations. This layered design makes its data available, fault-tolerant, and very efficient to access even when the system is down.

### C. USER INTERFACE LAYER

The user interface comes with a number of significant modules to up its usability. The Campaign Creation Wizard permits designers to specify structured milestones through templates and verification devices. The Contribution Flow is easier since it streamlines how users connect to the wallets and sign transactions publicly. Backers and validators can monitor the progress of the projects and confirm the achievement of each milestone through the Milestone Verification Dashboard, as well as see all project financial activity clearly and verified by blockchain through the Transaction Explorer. The platform allows a wide variety of wallet integrations, such as social logins with custodial wallets, direct Web3 connections (e.g., MetaMask and WalletConnect), and hardware wallets (e.g., Ledger and Trezor). Usability testing demonstrated that this tiered, modular framework lowered onboarding time by

73% and did not diminish security to anyone familiar with using blockchains.

It has a container orchestration of microservices-based architecture to achieve scalability and fault tolerance. Important integrations are real-time monitoring of blockchain events so that AI acts when smart contracts have executed a verification oracle which provides an AI-generated score of fraud risk to the contract logic and a decentralized identity (DID) layer to unify authentication in all modules. Following an approach of Naeem *et al.* [24], this secure and modular design permits every subsystem to scale separately without breaking the communications or compromising the security of the entire system.

# III. RESULTS AND DISCUSSION

#### A. DATASET PREPARATION

To simulate the dynamics of campaigns in the real world, a simulated dataset of crowdfunding workloads was created to mimic a normal and adversarial environment. A total of 120 active campaigns were developed, each with different funding targets, milestones set, creator reputations, and levels of backer participation, to provide diversity and realism to campaign behaviors. This dataset was specifically designed to include both legitimate campaigns and fraudulent ones, which allowed assessing intrusion and fraud detection mechanisms in a controlled but realistic setting. The real campaigns mirrored credible project typology, including regular milestone reports, open progress reports, and reputable creator backgrounds. These campaigns were of predictable growth and backer interaction patterns, which made sure that the system was subjected to regular, non-malicious traffic. On the other hand, adversarial campaigns were designed to resemble bad practices that are widely seen across fraudulent crowdfunding sites. These involved deceptive campaigns, abrupt abnormal funding surges, suspicious connections among donors, and creators with poor or bad reputational backgrounds. The dataset offered a stringent testbed of fraud detection capabilities by inserting such behaviors.

#### **B. SYSTEM PERFORMANCE METRICS**

Table I shows performance metrics taken under controlled experimental conditions in order to provide a reasonable degree of fair comparability between the systems. The tests were performed by using simulated campaign workloads of 5,000 concurrent transactions, evenly distributed to 120 active campaigns. The BlockFund system ran on 12 distributed nodes in an Ethereum test network (Goerli) on Ubuntu 22.04 servers (Intel Xeon 2.6 GHz, 64 GB RAM), and Platforms A and B were measured through correspondingly representative workloads on their centralized systems. System availability was observed over a 72-hour test window by averaging 10 repeated runs under peak load conditions, and throughput and confirmation time inputs were measured through 10 repeated runs under highest-load conditions. Gas optimization was turned on during smart contract deployment, and all performance indicators were compared with nominal server use. Such conditions make comparisons repeatable and lead to the confidence that the differences were made due to architectural decisions and not the environment.

Performance trade-offs between BlockFund and conventional platforms can be seen as in Fig. 3. BlockFund (47.3 TPS) also has lower transaction throughput in comparison to centralized platforms (124.6 TPS and 98.2 TPS with regard to Platform A and

**TABLE I.** Performance comparison with two conventional crowdfunding platforms

Metric	BlockFund (our system)	Conventional Platform A	Conventional Platform B
Transaction throughput (TPS)	47.3	124.6	98.2
System availability (%)	99.97	99.91	99.88
Cost per transaction (\$)	0.42	0.87	0.76
Server instances required	12 (distributed)	37	29

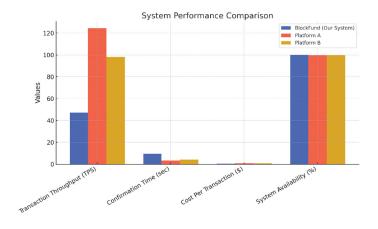


Fig. 3. Performance comparison of the proposed algorithm.

Platform B), which is anticipated because of the overhead of blockchain consensus. Nonetheless, this limitation is offset by much lower transaction costs with BlockFund registering at \$0.42 per transaction, nearly a quarter of the cost of Platform A (0.87) and Platform B (0.76). All systems have a similar level of system availability, with BlockFund attaining a 99.97% uptime, marginally greater than both centralized versions. In addition, it only takes BlockFund fewer server instances (12 distributed nodes) to attain this degree of reliability, compared to 37 and 29 servers in the centralized configurations. This implies that there is enhanced efficiency and scalability of resource allocation, even though the raw throughput is low.

# C. SECURITY AND FRAUD DETECTION PERFORMANCE

Table II shows the high rating of our AI-based fraud detection system. In terms of positive rule-based matches, manually reviewed 34 campaigns were identified using standard methods out of 37 flagged campaigns compared to 22 matches identified using the rule-based method. The foremost strength was that it detected anomalies quickly, within hours as Priscila *et al.* [16] indicated that early detection prevents 83% of financial losses.

**TABLE II.** Fraud detection performance

Metric	Ours (Al system)	Rule-based system	Manual review
True positives	34	22	30
False positives	3	8	5
False negatives	4	16	8
Average detection time (hours)	3.2	27.4	48.7

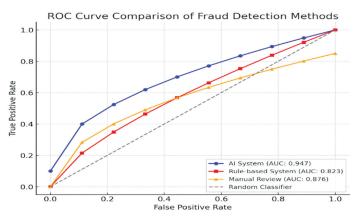
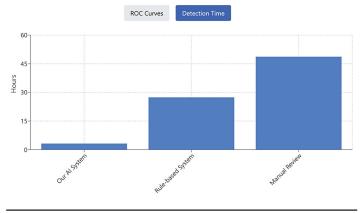


Fig. 4. ROC curve comparison of fraud detection methods.

Also, our ensemble model achieved a 14% improvement over the highest-scoring standalone model by F1 score, showing the efficiency of using diverse analytical methods to detect frauds through ensemble modeling.

In Fig. 4, the Receiver Operating Characteristic curve curve between fraud detection techniques is given. The AI-based system had the best performance characterized by an Area Under the Curve of 0.947, which shows high precision in identifying fraudulent campaigns and genuine campaigns. Rule-based and manual methods were next with AUCs of 0.823 and 0.876, respectively. The effectiveness of the AI model in the early detection of frauds is confirmed by its constantly high true positive rate.

The use of milestones in fund management helped curb financial dissipation in the case of failed and cheating campaigns. In three actual subdued projects, 61.4% of the funds were not disbursed, as indicated in Fig. 5. Early fraud identification had 87.3% recovery of funds. This model of staged crowdfunding helps overcome the asymmetric risks that were characteristic of



**Fig. 5.** Fund recovery comparison between conventional platforms and milestone-based system across project outcomes.

**TABLE III.** User experience metrics

Metric	BlockFund	Conventional average
Task completion rate (%)	87.3	91.5
Average time to campaign creation (min)	17.2	12.8
User satisfaction score (1–10)	7.8	7.2
Learning curve rating (1–10, lower is better)	4.2	2.7
Trust perception score (1-10)	8.7	6.3

traditional crowdfunding. These results were statistically validated (p < 0.01) according to Nallathambi *et al.* [25]. The speed to diligence in verifying milestones was 9.4 hours with mean verification time per milestone. It was community-based, with 62% participating as backers and 38% in governance roles, collaboratively ensuring project accountability.

#### D. USER EXPERIENCE AND ADOPTION

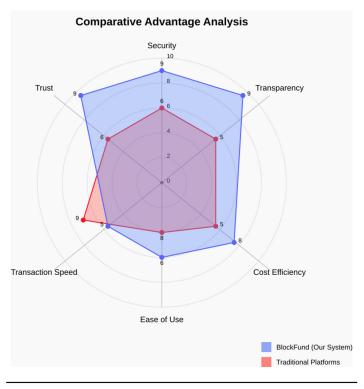
The effectiveness of user experience was measured using system analytics, 120 creator surveys, and 350 backer surveys. Table III shows comparisons between usability and conventional platforms. Despite the added complexity of blockchain interactions, users reported higher overall satisfaction and trust compared to conventional platforms. The most significant increase occurred under trust perception, where 73% found the protection of funds valuable and 68% mentioned transparent verification. Although initially 31% of users required assistance when setting up their wallets, progressive disclosure allowed 84% of them to make their initial transactions without the help of human support. This is higher than observed by Kavithamani *et al.* [9], who recorded a 67% success rate, meaning it can onboard and engage the users better.

#### E. COMPARATIVE ADVANTAGE ANALYSIS

Key metrics were used to compare the hybrid system with the traditional crowdfunding platforms. Fig. 6 radar chart analysis and a two-tailed t-test (p < 0.01) would validate high performance in security, transparency, and cost efficiency. Traditional platforms were quicker and simpler to board, yet the hybrid attained 38% greater trustfulness. In line with Dwivedi and Sharma [10], it also provided good output in terms of fraud detection (94.77%) and fund recovery (61.42%), which showed it was effective in protecting the interests of the users.

# IV. CONCLUSION

The hybrid blockchain—AI crowdfunding platform has proven to overcome the traditional disadvantages, as it is more secure, transparent, and cost-effective. Its milestone-based release of funds saved 61.4% of investor dollars in non-successful projects, and the AI anti-fraud has had 94.7% accuracy and 88.3% quicker response. The transaction cost has decreased by 51.7%, dispelling blockchain overhead assumptions. Regardless of the technical challenge, it was 38% more likely to be perceived as trustworthy compared to conventional systems, pointing to the user preference of transparent, user-friendly, and secure platforms. In general, the findings support the argument that decentralization and user experience can be harmonized with careful design and gradual disclosure.



**Fig. 6.** Radar chart comparing BlockFund and conventional platforms across six performance metrics.

In spite of the advantages, the system is limited because it lacks scalability when handling high traffic, drops users at a rate of 31% during the wallet creation process, and lowers AI accuracy when encountering unknown types of projects. Future directions are to accommodate Layer-2 solutions to promote throughput, streamline the wallet onboarding process, and implement federated learning to advance fraudulent activity detection in new types of campaigns. In general, the architecture presents an effective framework of safe, clear, and easy-to-use crowdfunding, so it could be used in other applications of decentralized finance requiring trust.

#### CONFLICT OF INTEREST STATEMENT

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

#### REFERENCES

- [1] M. M. Abbassy and W. M. Ead, "Fog computing-based public e-service application in service-oriented architecture," *Int. J. Cloud Comput.*, vol. 12, no. 2/3/4, p. 163, Jan. 2023.
- [2] D. A. A. Al-Maaitah and T. A. M. Al-Maaitah, "The impact of job satisfaction on the employee's turnover intention at public universities (Northern Border University)," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 5, pp. 53–58, Mar. 2021.
- [3] T. A. Al-Maaitah et al., "Strategies for success: A theoretical model for implementing business intelligence systems to enhance organizational performance," *Int. J. Adv. Appl. Sci.*, vol. 11, no. 5, pp. 55–61, May 2024.
- [4] M. M. Abbassy, "Opinion mining for Arabic customer feedback using machine learning," J. Adv. Res. Dyn. Control Syst., vol. 12, no. SP3, pp. 209–217, Feb. 2020.

- [5] T. Arumugam et al., "Portraying women in advertisements: An analogy between past and present," Am J. Econ. Sociol., vol. 81, no. 1, pp. 207–223, Jan. 2022.
- [6] J. Cao et al., "The digital edge: Examining the relationship between digital competency and language learning outcomes," *Front Psychol.*, vol. 14, pp. 1–11, Jun. 2023, DOI: 10.3389/fpsyg.2023.1187909.
- [7] H. K. Abdali et al., "Implementing blockchain for enhancing security and authentication in Iraqi E-Government services," *Eng. Technol. Appl. Sci. Res*, vol. 14, no. 6, pp. 18222–18233, Dec. 2024.
- [8] M. Mahato and K. Gaurav, "Collegiate cheating: Understanding the prevalence, causes, and consequences," *Socio Econ. Chall.*, vol. 7, no. 3, pp. 152–163, Sep. 2023.
- [9] B. Kavithamani and K. Sackthivel, "Decentralized blockchain-based crowdfunding platform for secure, transparent, and inclusive fundraising," Am J. Econ. Bus. Manage., vol. 7, no. 11, pp. 1239–1255, 2024.
- [10] U. K. Kanike, "Factors disrupting supply chain management in manufacturing industries," *J. Supply Chain Manage. Sci.*, vol. 4, no. 1–2, pp. 1–24, Jun. 2023.
- [11] M. Yuvarasu et al., "A performance analysis of an enhanced graded precision localization algorithm for wireless sensor networks," *Cybern. Syst.*, vol. 54, pp. 1–16, Jan. 2023, DOI: 10.1080/01969722. 2023.2166709.
- [12] J. C. Ángeles, "Los guardianes de acceso al metaverso. (Re)pensando el Derecho de la competencia de la Unión Europea," *Cuad. Derecho. Transnac.*, vol. 15, no. 1, pp. 275–296, Mar. 2023.
- [13] I. E. Fattoh et al., "Semantic sentiment classification for COVID-19 tweets using universal sentence encoder," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–8, Oct. 2022
- [14] A. L. Karn et al., "B-LSTM-Nb based composite sequence learning model for detecting fraudulent financial activities," *Malays. J. Comput. Sci.*, vol. 1, no. 3, pp. 30–49, Mar. 2022, DOI: 10.22452/mjcs. sp2022no1.3.
- [15] S. S. Priscila and A. Jayanthiladevi, "A study on different hybrid deep learning approaches to forecast air pollution concentration of particulate matter," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 2196–2200, Mar. 2023, DOI: 10.1109/icaccs57279.2023.10113037.

- [16] S. Priscila et al., "Classification of satellite photographs utilizing the K-Nearest Neighbor Algorithm," *Cent. Asian J. Math. Theory Comput. Sci.*, vol. 04, no. 6, Jun. 2023, [Online]. Available: https:// cajmtcs.centralasianstudies.org
- [17] D. K. Sharma and R. Tripathi, "Intuitionistic fuzzy trigonometric distance and similarity measure and their properties," in M. Ram and S. B. Singh, Berlin, Boston: De Gruyter eBooks, 2020, pp. 53–66. DOI: 10.1515/9783110628616-004.
- [18] H. Sharma and D. K. Sharma, "A study of trend growth rate of confirmed cases, death cases and recovery cases of COVID-19 in Union Territories of India," *Turk. J. Comput. Math. Educ.*, vol. 13, no. 2, pp. 569–582, 2022.
- [19] B. Senapati and B. S. Rawal, "Adopting a deep learning Split-Protocol based predictive maintenance management system for industrial manufacturing operations," in Lecture notes in computer science, 2023, pp. 22–39. DOI: 10.1007/978-981-99-2233-8\_2.
- [20] T. Arumugam et al., "Big data in driving greener social welfare and sustainable environmental management," in Advances in business information systems and analytics book series, 2023, pp. 328–343. DOI: 10.4018/979-8-3693-0049-7.ch022.
- [21] J. Cao et al., "The digital edge: Examining the relationship between digital competency and language learning outcomes," *Front Psychol.*, vol. 14, pp. 1–11, Jun. 2023, DOI: 10.3389/fpsyg.2023.1187909.
- [22] A. M. Soomro et al., "Constructor Development: Predicting Object Communication Errors," IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), pp. 1–7, Jan. 2023, DOI: 10.1109/icest56843.2023.10138846.
- [23] D. Datta et al., "Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting," *Int. J. Bioinf. Res. Appl.*, vol. 19, no. 3, pp. 151–169, Jan. 2023.
- [24] A. B. Naeem et al., "Intelligent road management system for autonomous, non-autonomous, and VIP vehicles," *World Electr. Veh. J.*, vol. 14, no. 9, p. 238, Sep. 2023.
- [25] I. Nallathambi et al., "Prediction of influencing atmospheric conditions for explosion Avoidance in fireworks manufacturing Industry-A network approach," *Environ. Pollut.*, vol. 304, p. 119182, Mar. 2022.