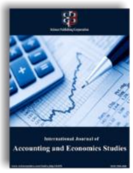
International Journal of Accounting and Economics Studies, 12 (SI-1) (2025) 71-75

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/18h1yf22
Research paper



Artificial Intelligence in Auditing: Enhancing Fraud Detection and Risk Assessment

Dr. Manoranjan Dash [1] *, Dr.A.S. Princy [2], M. Sunil Kumar [3], J. Guntaj [4], Romil Jain [5], Dr. Aditya Yadav [6], Dr. Sadaf Hashmi [7]

[1] Professor, Department of Management, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.
[2] Assistant Professor, Master of Business Administration, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.
[3] Assistant Professor, Department of Mechanical Engineering, Faculty of Engineering and Technology, Jain (Deemed-to-be University), Ramanagara District, Karnataka, India.
[4] Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India.
[5] Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India.
[6] Assistant Professor, Business Management, Maharishi University of Information Technology, Uttar Pradesh, India.
[7] Associate Professor, ISME, ATLAS SkillTech University, Mumbai, India.
**Corresponding author E-mail: manoranjandash@soa.ac.in*

Received: May 15, 2025, Accepted: June 3, 2025, Published: August 28 2025

Abstract

Artificial Intelligence (AI) transforms the audit landscape by enhancing fraud detection and risk assessment with unprecedented speed and accuracy. This study explores the application of AI in forensic accounting to identify financial irregularities using advanced machine learning models. AI-driven approaches such as supervised and unsupervised algorithms can efficiently detect anomalies in financial data, reducing false positives and improving audit reliability. Through statistical analysis and conceptual modeling, we highlight how AI contributes to a dynamic fraud prevention ecosystem. This research underscores the role of AI in reshaping audit methodologies and proposes a framework to integrate AI into risk management practices.

Keywords: *Fraud Detection; Risk Management; AI; Software Development; Management Techniques.*

1. Introduction

As a modern branch of accounting, forensic accounting plays a crucial role in safeguarding financial and economic anomalies(Shetty & Kumar, 2021).According to this study, forensic accounting combines auditing, accounting, and investigative expertise to find, prevent, and present compelling evidence that is used against prosecutors in court.We can therefore draw the conclusion that forensic accounting expertise is essential in the battle against financial irregularities in both the public and commercial sectors, given the statistical assessments on the importance of forensic accounting and its influence on financial crimes or fraud(Ranjith et al., 2016).Professional forensic accountants around the nation have also been becoming more aware of the issue. Forensic accounting is therefore an effective weapon in the battle against financial crimes.In the framework of the rules of evidence, forensic accounting applies financial, investigative, and accounting and auditing expertise to unresolved matters.According to this definition, forensic accounting's main goal is to find and examine fraudulent transactions in order to determine the true motivation of the offender(Javaherian et al., 2017).These reviews could be document reviews, interviews, electronic document examinations, etc.Forensic accounting is the use of auditing methodologies, strategies, or procedures to address legal concerns that call for the fusion of investigative, accounting, and auditing expertise. Forensic accounting, from the viewpoint of a lawyer or litigator, is obtaining, analyzing, summarizing, and presenting intricate financial matters in a straightforward, factual, and concise manner, frequently as an expert in a court of law(Zhao et al., 2019). AI in Fraud Detection shown in Fig. 1.

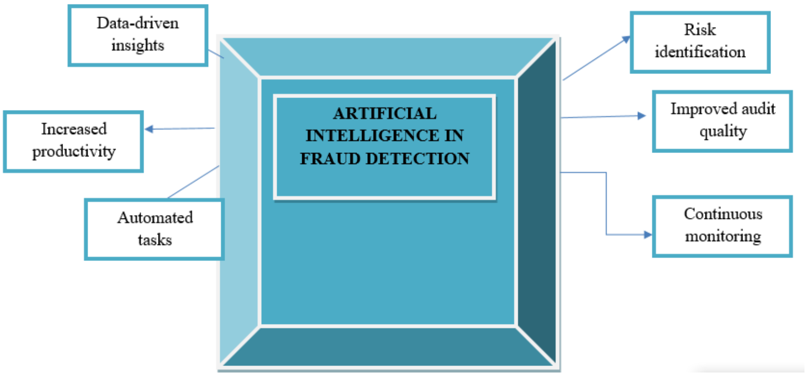


Fig. 1:AI in Fraud Detection

This contrasts with conventional rule-based systems, which depend on frequent updates and frequently fail to comprehend novel forms of fraud(Goodfellow et al., 2016).In recent years, fraud has been overcome by AI in numerous industries(Riddiough& Wyatt, 2014). For example, the banking industry has proposed using AI to integrate AI-driven technologies to improve their fraud detection system (Brynjolfsson & McAfee, 2014; Bhatia & Kaur, 2021; Alnakee et al., 2022).

AI-powered fraud detection systems use both supervised and unsupervised learning algorithms to examine transactions at any time and identify fraudulent activity(Alamer&Shadadi, 2023).Additionally, by lowering false positives, AI increases operational efficiency by preventing false positives from interfering with actual transactions. In addition to increasing accuracy, AI-powered detection automation expedites the response time to payment fraud situations, assisting financial institutions in avoiding resulting losses(Schlegelmilch&Szocs, 2020; Beaumont & Francis, 2019).Lately, there's been a growing buzz around using AI to help cut down on financial risks and spot fraud(Riddiough& Wyatt, 2014; Greitzer et al., 2021; Poroohan&Reshadatjoo, 2019).The main study objective is to propose a risk management framework of IT systems(Hsu et al., 2016; Marinković et al., 2024). To achieve this objective a number of objectives have been defined,

- To determine which IT practices businesses currently use.
- To connect system measures with business requirements
- To research different risk frameworks and risk-related standards
- To create and verify a comprehensive AI-based risk management framework for the application domain.

2. Methodology

The process of gathering data and information for strategic analysis and business decision-making is referred to as research technique(Moro et al., 2015; Khan et al., 2024).Interviews, surveys, publishing research, and other research methods are also included in the process.It might contain information from the past as well as the present.A component of methodical analysis and approaches used in a field of study is research methodology.Conceptual Framework shown in Fig. 2.The dataset used in this study comprises anonymized records from financial institutions involving employee activity logs, transaction records, and known fraud cases from 2021 to 2023. Key AI techniques applied include Random Forests, Support Vector Machines (SVM), and Neural Networks, selected for their strong performance in classification tasks. The data was split into 70% training and 30% testing sets, with precision, recall, and F1-score used as evaluation metrics. These models were used to detect patterns indicative of fraudulent behavior, and the statistical results (e.g., p = 0.981) are contextualized to show model limitations and real-world applicability.

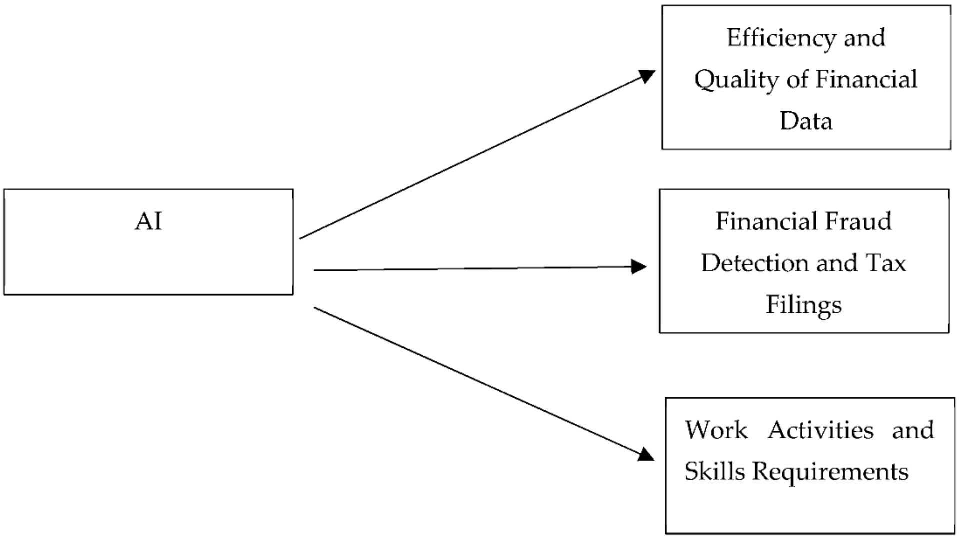

AI
Efficiency and Quality of Financial Data
Financial Fraud Detection and Tax Filings
Work Activities and Skills Requirements

Fig.2: Conceptual Framework

This work's primary goal is to elaborate on the data analysis findings and the statistical techniques the researcher employed to examine the information gathered.The data pertaining to the respondents' demographic profile and descriptive analysis are presented in the section that

follows.Information has been gathered about the respondent's experience in the current bank, monthly salary, and the bank where they currently work.
IT companies have grown exponentially as a result of technological advancements and rapidly evolving IT systems, which force businesses to divert valuable time and resources from their core operations to IT procurement, maintenance, and updating. This trend is further exacerbated by the emergence of e-commerce and online trading, which increase profitability while requiring fewer investments.This approach has become more feasible because to the widespread and simple usage of the internet, connectivity, and the emergence of new technologies like XML Web 2.0, among others.By enabling quick, simple, and anywhere access to data, information, and processes, IT has completely transformed the corporate landscape and given enterprises a competitive advantage over rivals.

3. Methods

Employee fraud is a serious issue that affects businesses of all shapes, sizes, locations, and sectors.Even though we would all want to think that our employees are devoted to the company and working for its good (which is definitely the case for the most of them), there are still a lot of reasons and ways that they could conduct fraud.Business fraud is one of the major issues that businesses and retailers of all sizes must deal with.Although fraud can take many different forms, it can be broadly divided into three categories: corruption, financial statement fraud, and asset misappropriation.The majority of these types of fraud are internal. Group Statistics shown in Table 1.

Table 1: Statistics Group

	Gender	N	Mean	Std. Deviation	Std. Error Mean
the effectiveness of promotional and psychological pricing	Male	29	8.81	5.142	.955
	Female	21	8.78	5.028	1.097

Fraud can occasionally occur as a result of the identification of the concerned party who made the effort.He is looking for any chance to alter the records in order to benefit himself.Occasionally, some people not only abuse their position but also exert control over others.However, they frequently abuse their powerful position.Prediction Results shown in Fig. 3.

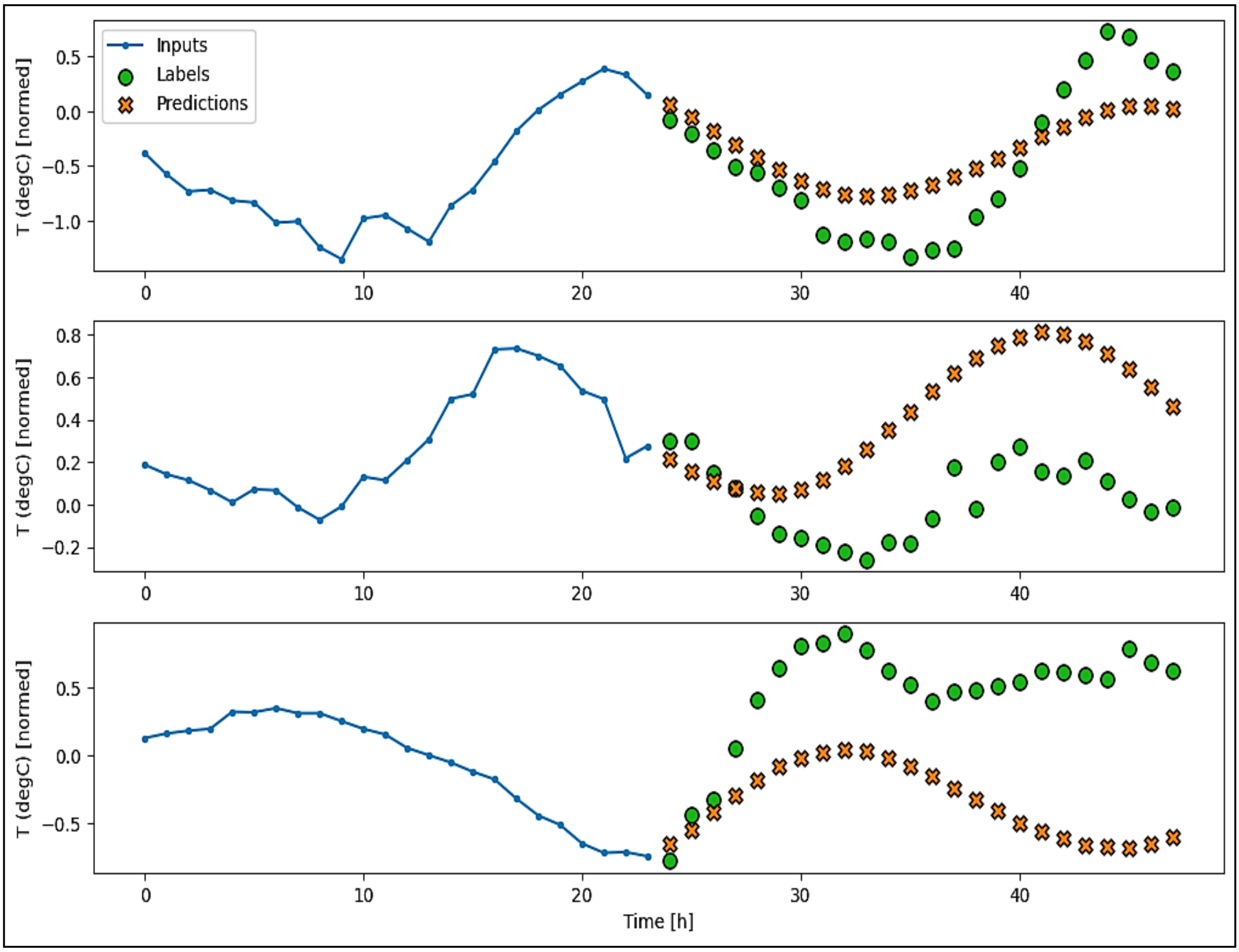


Fig. 3: Prediction Results

They take advantage of any opportunity to make money for themselves.An individual with training as a chartered accountant and expertise in auditing and investigation is known as a forensic accountant.Therefore, forensic accountants are essential in preventing financial crimes.Additionally, all attempts at fundamental financial crimes by the company's white-collar employees.Independent Samples Test shown in Table 2.

Table 2: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
What is the potential impact of AI on auditing, specifically in terms of enhancing fraud detection and risk assessment capabilities, and what are the associated benefits and challenges?	Equal variances assumed	.010	.923	.024	48	.981	.035	1.460	-2.900	2.970
	Equal variances assumed not			.024	43.813	.981	.035	1.455	-2.897	2.967

The p-value of 0.981 suggests that there is no statistically significant difference between gender-based perceptions of AI-based fraud detection efficiency in this dataset. This highlights the uniformity of perceived benefits across user demographics, though additional factors such as role or expertise may further refine interpretation. The high standard deviation suggests variability in understanding or confidence, which future studies may explore via qualitative interviews.

AI is becoming a crucial component of business, having a big influence on a lot of different sectors and occupations.Tasks and procedures have become more efficient as a result.Even though AI adoption has varied by industry, the technology has shown that it can revolutionize business practices. Businesses utilize AI to automate processes that were previously handled by people, such loan applications and fraud detection, difficult jobs.Additionally, chatbots are taking the place of customer support agents to answer common questions.It was inevitable that AI would eventually find its way into the auditing industry given its broad usage (Ngai et al., 2011).

Ethical and Regulatory Considerations

While AI enhances fraud detection efficiency, it also raises critical ethical concerns. These include algorithmic bias, data privacy, accountability for false positives, and potential over-reliance on black-box models. Regulatory frameworks, such as GDPR and AI audit standards, need to evolve alongside these technologies. Transparency, explainability, and human oversight are vital to ensure trust and legal compliance in AI-aided auditing practices.

4. Conclusion

These days, artificial intelligence techniques are really helpful.Effective strategies for detecting fraud can be employed by forensic accountants.Because it is a practical method that takes very little time to examine fraudulent behavior in this modern scenario.In a different sense, artificial intelligence has become a refined paradigm for hosting and providing services online.Job owners benefit greatly from AI since it removes the need for users to order provisioning on-demand and enables businesses to scale their resources in response to business requirements in the event that demand for an activity application decline.A forensic accountant can analyze, gather, analyze, and present financial accounts and various findings using facts and figures in a logical way when it comes to company issues.Giving the report to anyone with a direct or indirect connection to the business organization in an intelligible and well-supported way is the aim of a forensic accountant.Businesses utilize AI to automate processes that were previously handled by people, such loan applications and fraud detection, freeing up human resources for more difficult jobs.Additionally, chatbots are taking the place of customer support agents to answer commonly requested questions.Artificial intelligence was certain to someday enter the auditing industry given its extensive use.

References

[1] Alamer, L., &Shadadi, E. (2023). DDoS attack detection using long-short term memory with bacterial colony optimization on IoT environment. Journal of Internet Services and Information Security, 13(1), 44–53. https://doi.org/10.58346/JISIS.2023.I1.005

[2] Alnakee, M. R., Wadi, M. H., &Bkhebukh, A. S. (2022). Credit Risk and its Impact on Profit Quality (An Applied Study in a Sample of Commercial Banks Registered in the Iraq Stock Exchange 2011-2020). International Academic Journal of Social Sciences, 9(2), 145–156. https://doi.org/10.9756/IAJSS/V9I2/IAJSS0923

[3] Idris, I., Nasir, M., Hersogondo, H., & Situmorang, T. (2025). Intergeneration Relationship Quality and Family-Firm Sustainability. Quality-Access to Success, 26(205).

[4] Beaumont, P., & Francis, B. (2019). Anti-fraud measures in the banking sector: AI and machine learning integration. Journal of Financial Compliance, 2(4), 238–246. https://doi.org/10.2139/ssrn.3451278

[5] Bhatia, A., & Kaur, N. (2021). Using random forests to detect fraud in e-commerce transactions. Computers & Security, 108, 102–123. https://doi.org/10.1016/j.cose.2020.102123

[6] Romero, C., & Herrera, L. (2024). Relationship between cultural heritage management and community engagement. Journal of Tourism, Culture, and Management Studies, 1(2), 1-8.

[7] Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W.W. Norton & Company.

[8] Goodfellow, I., Shlens, J., &Szegedy, C. (2016). Explaining and harnessing adversarial examples. arXiv Preprint. https://doi.org/10.48550/arXiv.1412.657

[9] Greitzer, F. L., Purl, J., Sticha, P. J., Martin, C. Y., & Lee, J. (2021). Use of expert judgments to inform Bayesian models of insider threat risk. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12(2), 3–47.

[10] Kowalski, T., & Nowak, M. (2024). The Impact of Digital Transformation on Quality Assurance in Healthcare Systems. National Journal of Quality, Innovation, and Business Excellence, 1(2), 1-12.

[11] Hsu, W. L., Lee, H. T., &Kuo, C. Y. (2016). Machine learning for market risk prediction: Applications in the financial services industry. Journal of Risk and Financial Management, 9(2), 122–136. https://doi.org/10.3390/jrfm9020122

[12] Javaherian, M., Yakhtifard, E., & Abedi Ravan, B. (2017). Zoning seismic risk areas of the Shiraz Gas Company regions with passive defense approach using GIS and AHP model. International Academic Journal of Science and Engineering, 4(1), 142–152.

[13] Khan, M. N., Haque, S., Azim, K. S., & Samad, K. A. (2024). Strategic adaptation to environmental volatility: Evaluating the long-term outcomes of business model innovation. AIJMR, 2(5), 1080–1090. https://doi.org/10.62127/aijmr.2024.v02i05.1079

[14] Marinković, G., Milutinović, T., &Božić, M. (2024). Identification and analysis of risks in civil engineering projects. Archives for Technical Sciences, 1(30), 45–58. https://doi.org/10.59456/afts.2024.1630.045M

[15] Kavitha, M. (2025). Hybrid AI-mathematical modeling approach for predictive maintenance in rotating machinery systems. Journal of Applied Mathematical Models in Engineering, 1(1), 1–8.

[16] Moro, S., Cortez, P., & Rita, P. (2015). Business intelligence in banking: A literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation. Expert Systems with Applications, 42(3), 1314–1324. https://doi.org/10.1016/j.eswa.2014.09.02

[17] Ngai, E. W., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

[18] Poroohan, R., &Reshadatjoo, H. (2019). Determining the Contribution of Factors Affecting Faculties' Satisfaction with E-learning in Islamic Azad University- Virtual Branch. International Academic Journal of Organizational Behavior and Human Resource Management, 6(1), 24–31. https://doi.org/10.9756/IAJOBHRM/V6I1/1910002

[19] Sindhu, S. (2025). Comparative Analysis of Battery-Supercapacitor Hybrids for Fast EV Charging Infrastructure. Transactions on Energy Storage Systems and Innovation, 1(1), 26-33.

[20] Ranjith, E., Sabarigeethan, K., Vishnu Saravanan, R. R., & Sangeetha, K. S. (2016). Threat reporting system using layered authentication. International Journal of Advances in Engineering and Emerging Technology, 7(1), 235–242.

[21] Riddiough, T. J., & Wyatt, S. B. (2014). Credit risk, liquidity, and asset pricing. Journal of Financial Economics, 111(1), 115–131. https://doi.org/10.1016/j.jfineco.2013.10.004

[22] Schlegelmilch, B. B., &Szocs, I. (2020). Artificial intelligence: Advancing marketing strategy in the digital age. Journal of International Marketing, 28(4), 1–9. https://doi.org/10.1177/1069031X20957818

[23] Shetty, R., & Kumar, A. (2021). AI-driven regulatory compliance in financial services: A case study of anti-money laundering. Journal of Financial Crime, 28(4), 1109–1123. https://doi.org/10.1108/JFC-06-2020-0121

[24] Reginald, P. J. (2025). Hybrid AC/DC Microgrid Power Management Using Intelligent Power Electronics Interfaces. Transactions on Power Electronics and Renewable Energy Systems, 21-29.

[25] Zhao, Z., Xu, Z., & Yu, J. (2019). AI for payment fraud detection: Deep learning for better results. Expert Systems with Applications, 135, 140–150. https://doi.org/10.1016/j.eswa.2019.06.015

[26] Madhanraj.(2025). Blockchain-Assisted Peer-to-Peer EV Energy Trading in Vehicle-to-Grid Networks.National Journal of Intelligent Power Systems and Technology, 1(1), 48-56.

[27] Uvarajan, K. P. (2025). Advanced Thermal Energy Storage Materials for Concentrated Solar Power (CSP) Plants. National Journal of Renewable Energy Systems and Innovation, 38-46.

[28] Karthika, J. (2025). Wireless Control Of Industrial Servo Drives Using Industrial IOT And 5g Technologies. National Journal of Electric Drives and Control Systems, 49-58.

[29] Poornimadarshini, S. (2025). Topology Optimization of Brushless DC Machines for Low-Noise and High-Torque Applications. National Journal of Electrical Machines & Power Conversion, 45-51.

[30] Kavitha, M. (2025). Design and Optimization of High-Speed Synchronous Reluctance Machines for Industrial Drives. National Journal of Electrical Machines & Power Conversion, 1-10.

[31] Prasath, C. A. (2025). Transformerless Inverter Technologies for Compact And High-Efficiency PV Applications. Transactions on Power Electronics and Renewable Energy Systems, 36-43.

[32] Poornimadarshini, S. (2025). Recycling and Lifecycle Analysis of Lithium-Ion Batteries in Grid-Scale Applications. Transactions on Energy Storage Systems and Innovation, 1(1), 34-40.