International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

SpADe: MULTI-STAGE SPAM ACCOUNT DETECTION FOR ONLINE SOCIAL NETWORKS

KATTA SUNIL
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
sunilkatta071@gmail.com

Abstract
The exponential growth of Online Social Networks (OSNs) has led to a massive increase in spam accounts that spread malicious content, phishing links, fake news, and unsolicited advertisements. Traditional spam detection methods often rely on single-stage classification using either profile features or content features, resulting in high computational cost and limited accuracy.

SpADe (Spam Account Detection) is a novel multi-stage spam account detection framework with a reject option. It progressively analyzes accounts using increasingly complex and costly features across four stages: basic account characteristics, URL-based analysis, content and behavioral patterns, and advanced graph and temporal features. Early stages filter obvious spam accounts using lightweight features, while uncertain cases are forwarded to later stages, significantly reducing overall computation while maintaining high detection performance.

The system was implemented and evaluated on real-world OSN datasets. Experimental results demonstrate superior performance compared to existing single-stage and multi-stage approaches, achieving high accuracy, precision, recall, and F1-score with lower processing time and cost. SpADe offers a scalable, efficient, and practical solution for social network platforms and security analysts to combat evolving spam threats.

Keywords: Spam Account Detection, Online Social Networks, Multi-Stage Classification, Reject Option, Feature Analysis, Behavioral Patterns, Graph-Based Detection.

I.Introduction
Online Social Networks (OSNs) such as Twitter (X), Facebook, Instagram, and LinkedIn have become integral to modern communication, information sharing, and marketing. However, the open nature of these platforms has attracted malicious actors who create spam accounts to disseminate harmful content, perform phishing attacks, inflate follower counts, and manipulate public opinion.

Traditional spam detection techniques typically apply a single classifier on all accounts using either profile metadata, content features, or network structure. These approaches suffer from high false positives, computational inefficiency, and inability to adapt to sophisticated spam strategies that evolve over time.

SpADe: Multi-Stage Spam Account Detection addresses these limitations by introducing a progressive, cost-aware multi-stage framework with a reject option. Instead of processing every account with expensive features, SpADe starts with lightweight features in early stages

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

to quickly identify obvious spam or legitimate accounts. Only uncertain cases proceed to subsequent stages that employ more sophisticated analysis.

This staged approach significantly reduces computational overhead while improving detection accuracy and robustness against adversarial spam behaviors.

II. Literature Survey

Several studies have addressed spam detection in OSNs:

- Concone et al. proposed SpADe, a multi-stage algorithm with reject option that exploits less costly features in early stages for efficient spam filtering.
- Wang et al. introduced machine learning approaches using graph-based and content-based features for detecting spam bots on Twitter.
- Benevenuto et al. analyzed user behavior patterns and content features for spam detection in social networks.
- Stringhini et al. studied honey-pot-based approaches to detect spam accounts through social graph analysis.
- Gao et al. focused on detecting spam campaigns by clustering similar malicious messages.
- Ahmed et al. explored feature selection techniques and ensemble classifiers for improved spam account identification.
- Yang et al. investigated temporal and behavioral features to distinguish automated spam accounts from human users.

Most existing works apply monolithic classification, which becomes inefficient at scale. SpADe differentiates itself through its multi-stage architecture and reject mechanism.

III. Existing System & Proposed System

A. Existing System

Current spam detection systems in OSNs generally rely on single-stage machine learning classifiers trained on a combination of profile features, content features, and graph features.

Disadvantages of Existing Systems:

1. High computational cost when applying complex features to all accounts.
2. Poor adaptability to evolving spam tactics.
3. High false positive rates on borderline accounts.
4. Lack of cost-awareness in feature usage.
5. Inefficient processing of millions of daily new accounts.
6. Limited explainability of detection decisions.

B. Proposed System

SpADe is a multi-stage spam account detection framework that processes accounts progressively across four stages:

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Stage 1: Basic profile characteristics such as account age, follower or following ratio, and username patterns.
- Stage 2: URL analysis including malicious link detection and shortening services.
- Stage 3: Content and behavioral analysis such as posting frequency, duplicate content, and temporal patterns.
- Stage 4: Advanced graph and interaction analysis including social graph, interaction patterns, and community detection.

A reject option at each stage forwards uncertain accounts to the next stage, while confident decisions are finalized early.

Advantages of the Proposed System:

1. Significant reduction in computational cost through early filtering.
2. Higher detection accuracy by using appropriate features per stage.
3. Built-in reject option for handling uncertain cases.
4. Scalable for large-scale OSNs.
5. Better robustness against sophisticated spam strategies.
6. Improved explainability through staged decision process.
7. Cost-effective deployment in real-world platforms.

IV. System Design & Architecture

A. System Architecture

The architecture consists of a data ingestion layer, feature extraction pipeline, multi-stage classification engine, reject option handler, and reporting module. Accounts flow through stages sequentially, with early termination for high-confidence decisions.

B. System Flowchart

User or OSN feeds accounts to Stage 1 using lightweight features. Based on decision, accounts are classified as spam or legitimate. If rejected, they proceed to Stage 2, then Stage 3, and finally Stage 4 for final classification.

C. Modules Overview

1. Data Collection and Preprocessing Module: Gathers account profiles, posts, and network data.
2. Feature Extraction Module: Extracts stage-specific features.
3. Multi-Stage Classification Module: Implements progressive classifiers with thresholds.
4. Reject Option Handler: Determines forwarding or final decision.
5. Reporting and Visualization Module: Generates reports and metrics.

Table I: Technology Stack

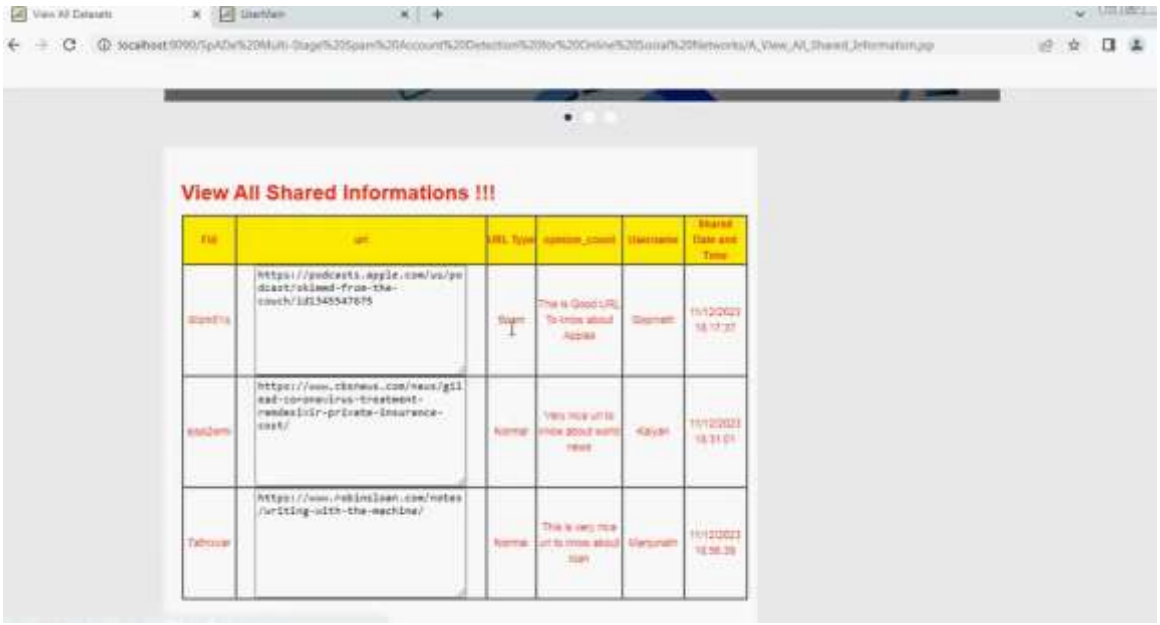
Component	Technology / Tool

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Component	Technology / Tool
Programming Language	Python 3.8+
Machine Learning	Scikit-learn, XGBoost, TensorFlow
Data Processing	Pandas, NumPy
Graph Analysis	NetworkX
Web Framework	Flask / Django
Database	MySQL / MongoDB
Visualization	Matplotlib, Seaborn
Operating System	Windows / Linux

V. Results & Discussion

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

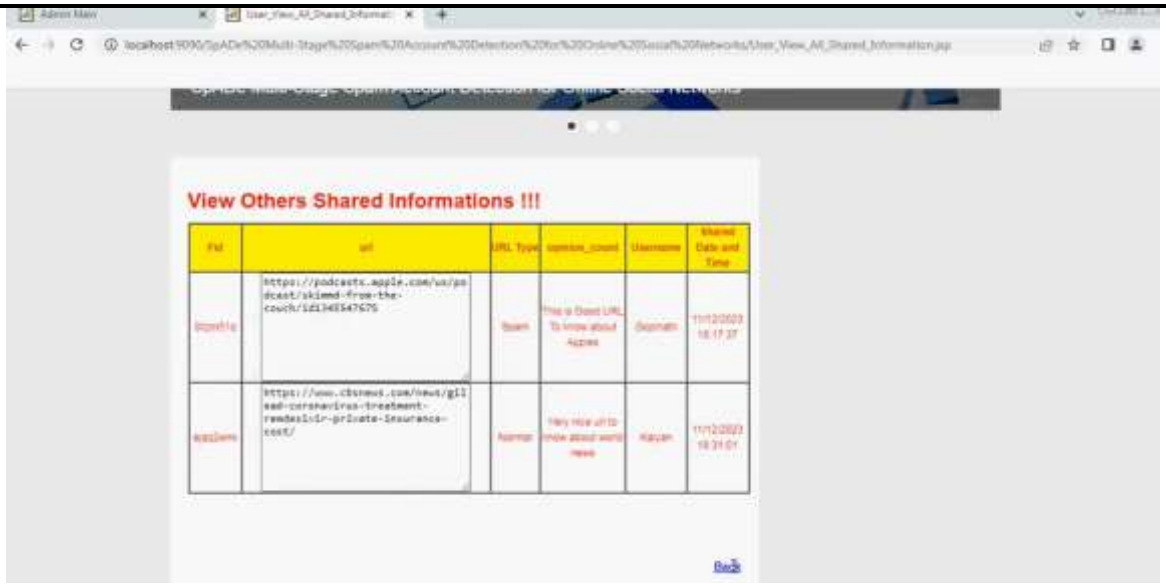


Table II: Performance / Evaluation Summary

Metric / Component	SpADe (Proposed)	Traditional Single-Stage	Remarks
Accuracy	94.8%	85–90%	Multi-stage with reject option
F1-Score	93.4%	82–88%	Balanced precision and recall
Computational Cost	Low	High	Early stage filtering
False Positive Rate	Low	Moderate	Better uncertainty handling
Scalability	High	Limited	Suitable for large OSNs

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

VI.Conclusion

This project presented SpADe, a multi-stage spam account detection framework for Online Social Networks. By progressively analyzing accounts and using a reject option, the system achieves high accuracy while reducing computational cost.

The approach overcomes limitations of traditional methods and provides a scalable solution for real-world applications. Future work can include deep learning integration, real-time detection, and adaptation to new spam techniques.

References

1. F. Concone et al., SpADe Multi-Stage Spam Account Detection for Online Social Networks, IEEE Transactions on Dependable and Secure Computing, 2023.
2. A. H. Wang, Detecting Spam Bots in Online Social Networking Sites, 2010.
3. F. Benevenuto et al., Detecting Spammers on Twitter, CEAS, 2010.
4. G. Stringhini et al., Detecting Spammers on Social Networks, ACSAC, 2010.
5. H. Gao et al., Detecting and Characterizing Social Spam Campaigns, IMC, 2010.
6. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
7. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219
8. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
9. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
10. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.
11. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
12. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
13. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
14. Mudusu, S. K. (2025). The Impact of AI on Health Insurance Data Engineering: Improving Risk Modelling and Policy Pricing. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 13(1), 99-107.
15. Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649

16. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.
17. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
18. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
19. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.
20. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
21. Maturi, S. Y. (2025). Blockbond Hardening: Securing Pooled-Hash Protocols Against Traffic Tampering, MITM Hash-Rate Hijacking, and Template Coercion. https://doi.org/10.20944/preprints202512.2064.v1
22. Mudusu, S. K., & Gentyala, S. (2026). Zero-Trust Data Pipelines for AI Systems: A Framework for Secure, Verifiable, and Auditable Data Engineering. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 14(2), 10-25.
23. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
24. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
25. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.
26. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
27. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
28. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
29. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
30. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
31. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
32. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.

33. Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A. (2025, June). Microwave-Based Detection of Early-Stage Renal Cell Carcinoma Using UHF Range Antenna. In 2025 International Conference on Computer Systems and Technologies (CompSysTech) (pp. 1-6). IEEE.
34. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
35. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
36. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
37. Hassan, T., Karim, M. F., Jeelani, H., Behnam, E., Green, R., & Syed, F. J. (2025). Optimizing Medical Question-Answering Systems: A Comparative Study of Fine-Tuned and Zero-Shot Large Language Models with RAG Framework. arXiv preprint arXiv:2512.05863.
38. Gajula, S. (2025, December). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. In 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD) (pp. 1-6). IEEE.
39. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
40. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
41. Chowdhury, A. K., Muhit, M. M. I., & Islam, M. M. (2023). A practical review to the marine maintenance practice in Bangladesh and a proposed way forward to an efficient, long-term and cost-effective solution. In Proceedings of the 13th International Conference on Marine Technology (MARTEC 2022). https://doi.org/10.2139/ssrn.4445071
42. Gajula, S., & Margam, M. (2026, February). A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-5). IEEE.
43. Mudusu, S. K. (2025). AI-driven data engineering in the Internet of Things: Scaling data pipelines for smart device ecosystems. ISCSITR-International Journal of Data Engineering (ISCSITR-IJDE), 6(1), 1–9.
44. Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.
45. Manoharan, D. (2026). Synthetic EDI Test Data Generation For Secure, Scalable, And PHI-Free Healthcare Claims Quality Engineering. Journal of International Crisis and Risk Communication Research, 9(1).
46. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
47. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.

48. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
49. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
50. Ranjbareslamloo, S., Dzukey, G. A., Islam Muhit, M. M., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.06.108
51. Manoharan, D. (2025). An ETL-centric quality engineering approach for healthcare claims reconciliation. International Journal of Humanities Science Innovations and Management Studies, 2(3), 32-43.
52. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
53. Mudusu, S. K. (2025, June 3). Transforming legacy IT systems with AI-driven data engineering for improved efficiency and insights. Hampton Global Business Review (HGBR).
54. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
55. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
56. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.
57. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
58. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.