iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** III **Month of publication:** March 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.78839

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

# Adaptive Engine for General Intelligence Security AI-Based Multi-Layer Cybersecurity System

M.S.S.V.G. Manikanta[1], Dangeti Rajkumar[2], A.S.R. Karthikeya[3], Sape Sunny[4], Chavatapalli Tatayya Naidu[5]
[1, 2, 3, 4]*Department of CSE(AIML), Bonam Venkata Chalamayya Engineering College, Andhra Pradesh, India*
[5]*Assistant Professor, Department of CSE(AIML), Bonam Venkata Chalamayya Engineering College, Andhra Pradesh, India*

***Abstract:*** ***The rapidly evolving cybersecurity landscape demands intelligent, multi-modal, and explainable threat detection systems. With over 3.5 billion Android devices worldwide and millions of new malware samples appearing every year, traditional signature-based tools have become increasingly ineffective. Moreover, modern cyber threats do not arrive through a single channel — attackers exploit Android applications, malicious documents, phishing URLs, and harmful content simultaneously, yet most available tools address only one of these vectors at a time. This project presents AEGIS 2026 (Adaptive Engine for General Intelligence Security), a production-ready, AI-powered multi-layer cybersecurity platform engineered to detect threats across four distinct modalities: Android APK malware, malicious documents (PDF, DOCX, XLSX), phishing and malicious URLs, and harmful text content. The system is built on a soft-voting ensemble of XGBoost and Random Forest classifiers trained on 54+ static features extracted using the androguard library, achieving a test accuracy of 96.3 The platform is deployed as a secure Flask REST API exposing 14 endpoints, with engineering controls including rate limiting (50 requests/hour/IP), werkzeug secure file handling, SHA-256-keyed LRU caching, SQLite persistence for scan history, and automated forensic PDF report generation via ReportLab. A browser-based Single Page Application (SPA) dashboard with Chart.js visualisations and voice alert capability completes the user-facing interface. AEGIS addresses five documented limitations of existing tools signature dependency, single-modality coverage, black-box AI decisions, absence of production engineering, and string-match false positives — and outperforms all compared baseline systems across every measured metric.***

***Index Terms: Android Malware Detection, Explainable AI, SHAP, XGBoost, Random Forest, Phishing Detection, Document Threat Detection, Content Moderation, Flask REST API, androguard, Multi-Layer Cybersecurity.***

## I. INTRODUCTION

AEGIS 2026 (Adaptive Engine for General Intelligence Security) is a Final Year B.Tech project that implements a complete, production-ready, AI-driven multi-layer cybersecurity platform. The project was conceived to address a well-documented gap in the current cybersecurity tooling landscape: the absence of a unified, open-source, machine-learning-based system that can simultaneously analyse Android applications, malicious documents, phishing URLs, and harmful text content while providing transparent, explainable AI decisions. The system is not merely a research prototype — it is engineered as a deployable web application with a Flask REST API backend, a browser-based dashboard frontend, and a full supporting stack including database persistence, caching, rate limiting, and professional PDF report generation. This approach demonstrates mastery not only of machine learning algorithms but also of software engineering, cybersecurity principles, and system design.

AEGIS comprises four primary detection engines:

*1)* APK Scanner — detects Android malware using static analysis of 54+ features extracted from the APK file using the androguard library, processed by an XGBoost + Random Forest ensemble with SHAP explainability.
*2)* Document Threat Scanner — analyses PDF, DOCX, XLSX, and PPTX files for malicious macros, embedded scripts, exploit keywords, and suspicious structural patterns.
*3)* URL/Phishing Scanner — classifies URLs using 30+ lexical and structural features to detect phishing, brand impersonation, domain generation algorithm (DGA) activity, and malware distribution links.
*4)* Content Moderation Engine — scans plain text for PII exposure, toxicity, hate speech, and embedded malware code patterns.

All four engines feed into a common output schema and are accessible via a unified REST API, a web dashboard, and an automated PDF forensic report generator.

©IJRASET: All Rights are Reserved 

### A. *Problem statement*

The cybersecurity domain faces five interconnected challenges that AEGIS is specifically designed to address:

Classical antivirus products maintain databases of known malware signatures. Polymorphic, metamorphic, and packed malware variants modify their code structure with each replication cycle, rendering signature matching ineffective. Zero-day malware — malware that has never been observed before evades all signature-based defences entirely. A machine learning approach that learns behavioural patterns rather than fixed signatures is essential

Existing tools are purpose-built for a single threat type: VirusTotal for file/URL hashes, DREBIN for APKs, URLVoid for URLs, ClamAV for file signatures. Modern attacks combine multiple vectors simultaneously — a phishing email containing a malicious document linking to a malware-hosting URL that delivers an APK. No single open-source tool can holistically analyse all four threat vectors in one workflow.

Where ML-based tools exist, they function as black boxes: they return a SAFE or MALWARE verdict without explaining which features drove the decision. Security analysts cannot act on opaque decisions with confidence. The EU AI Act (2024) and NIST AI RMF both require high-risk AI systems to provide meaningful explanations to affected users and oversight teams.

Many APK scanners detect suspicious API usage by searching for dangerous API strings in decompiled code. This approach has an 18.7 percent false positive rate because legitimate applications may import libraries that reference dangerous APIs without ever calling them.

### B. *Existing Approaches*

The web dashboard provides a drag-and-drop file upload interface — no command-line knowledge is required from end users.The REST API design follows industry-standard REST-ful conventions, enabling integration into existing security workflows without modification to the AEGIS codebase.SHAP feature attribution and LLM-generated plain-English explanations make the AI output accessible to analysts who are not data scientists.

For academic or small-scale deployment, a standard PC or a basic cloud VM (5–20rs per month) is sufficient.No commercial software licences are required.The estimated total cost of the project is within 0–5rs,000 (domain/hosting only if publicly deployed).

## II. LITERATURE REVIEW

This chapter reviews the existing literature on cybersecurity systems, malware detection approaches, and AI-based security research to contextualise the contributions of AEGIS and demonstrate awareness of the prior art. VirusTotal is a free online service owned by Google that aggregates scan results from over 70 antivirus engines for submitted files, URLs, and domains. While it provides broad signature-based coverage and is widely used by security researchers, it does not perform machine learning-based analysis, does not provide feature-level explanations for its verdicts, and does not support simultaneous analysis of multiple threat modalities (APK + document + URL + text) through a single API call. Its public API is also rate-limited to 4 requests per minute on the free tier.

ClamAV is an open-source, signature-based antivirus engine maintained by Cisco Talos. It is widely deployed in enterprise mail gateways and Linux servers. ClamAV relies entirely on signature databases (ClamAV definition files) and cannot detect zero-day or polymorphic malware variants that do not match a known signature. It provides no explainability, no REST API, and no web interface in its base form.

URLVoid is a web service that checks URLs against multiple reputation databases and DNS blacklists. It performs no machine learning analysis and relies entirely on blacklisting — a reactive approach that cannot detect new phishing domains that have not yet been reported. URLhaus (by abuse.ch) maintains a database of malware-hosting URLs but again operates on a blacklist model rather than behavioural classification.

DREBIN is a landmark paper in static Android malware detection. The authors extracted features from AndroidMan-ifest.xml files and disassembled DEX bytecode, including permissions, API calls, network addresses, and used hardware features. A linear SVM was trained on a dataset of 123,453 applications (5,560 malware, 123,453 benign), achieving 94 percent detection accuracy with a false positive rate of 1 percent. DREBIN's key limitation is its vulnerability to adversarial manipulation — by appending benign features to malicious APKs, an attacker can reduce DREBIN's detection rate significantly (Grosse et al., 2017). DREBIN is also a research prototype with no web interface, API, or deployment infrastructure.

MaMaDroid modelled sequences of API calls in Android applications as Markov chains, capturing higher-order behavioural patterns that are invisible to feature-counting approaches. It achieved 99 percent accuracy on a restricted dataset. However, MaMaDroid requires API call sequences extracted from the execution of the application — a dynamic analysis requirement — making it computationally expensive and unsuitable for pre-installation static scanning.

Maiorca et al. proposed an ML approach for detecting malicious PDF files using structural features from the PDF object tree. Their system achieved 99.52 percent accuracy on a controlled dataset but addressed only the PDF format and was subsequently shown to be vulnerable to mimicry attacks where malicious PDFs are padded with benign-looking objects.

The integration of Large Language Models (LLMs) into cybersecurity tooling has accelerated since the public release of GPT-4 (2023) and Meta LLaMA 3 (2024). Applications include natural language threat report generation, vulnerability explanation, and incident response guidance. AEGIS integrates Ollama LLaMA 3 as a local inference server, enabling LLM-powered natural language explanations without data privacy concerns associated with cloud-based LLM APIs.

### *A. Proposed System*

AEGIS addresses every documented limitation through a unified, engineered solution: • Explainability: SHAP TreeEx-plainer + Ollama LLaMA 3 provide both technical (feature attribution) and non-technical (plain English) explanations for every scan. • Multi-Modal Coverage: Single API supporting APK, document, URL, and text inputs through a common interface. • ML-Based Detection: XGBoost + Random Forest ensemble learns malware behavioural patterns rather than fixed signatures — effective against polymorphic and zero-day variants. • Production Engineering: Rate limiting, secure file handling, LRU caching, SQLite persistence, and PDF reporting are built in. • Call-Graph API Detection: androguard xref analysis reduces false positive rate from 18.7• Professional Reporting: ReportLab PDF reports with full SHAP attribution, IOC list, VirusTotal results, and AI explanation. • VirusTotal Integration: Every scan enriched with 70+ AV engine verdicts via VirusTotal API v3.

- Production-ready engineering — deployable with no additional development. • LLM natural language explanations bridge the gap between technical ML output and non-technical

| | |
|---|---|
| **TIER 1 Presentation** | **Browser-based Single Page Application (SPA)**<br>Components: Drag-drop upload zone • Scan results dashboard • SHAP attribution chart (Chart.js) • Live threat feed panel • AI explanation panel • Voice alert (Web Speech API) • PDF download button<br>Technology: HTML5, CSS3, Vanilla JavaScript, Chart.js, Fetch API |
| **TIER 2 Application** | **Flask REST API Server**<br>Components: 14 REST endpoints • Rate limiter (Flask-Limiter) • Secure file upload handler • Route dispatcher • SHA-256 LRU cache • SQLite persistence layer • PDF report generator<br>Technology: Python Flask 3.x, werkzeug, python-dotenv |
| **TIER 3 Intelligence** | **ML Engine + Feature Analysis Pipeline**<br>Components: androguard APK parser • 54+ feature extractor • Call-graph xref API detector • XGBoost + RF VotingClassifier • SHAP TreeExplainer • Document parser (PyMuPDF / python-docx / openpyxl) • URL lexical feature extractor • NLP content moderation pipeline<br>Technology: androguard, scikit-learn, XGBoost, SHAP, PyMuPDF, python-docx |
| **TIER 4 External** | **External Services + Storage**<br>Components: VirusTotal API v3 (REST, async) • Ollama LLaMA 3 (local LLM server) • SQLite database file • SHA-256 LRU in-memory cache<br>Technology: requests, sqlite3, functools.lru_cache, Ollama API |

Fig. 1. Four-Tier System Architecture

stakeholders. • Open-source and free — no licensing costs for academic or research use.

### *B. System Architecture*

*AEGIS* follows a four-tier layered architecture, separating concerns between user interaction, application logic, intelligence processing, and external service integration. This design pattern maximises modularity, enables independent testing of each tier, and *facilitates future* scaling. The frontend is a Single Page Application (SPA) that communicates with the Flask backend exclusively through asynchronous REST API calls (JavaScript Fetch API). No page reloads occur during normal operation — all *state* transitions are handled in JavaScript. Upload Zone A drag-and-drop file upload zone built with HTML5 FileReader API and CSS3 transitions. Users can either drag a file into the drop zone or click to open a file picker dialog. The accepted file types are indicated (APK, PDF, DOCX, XLSX, PPTX). File size is validated client-side before submission. Results Dashboard Upon completion of a scan, the results panel is dynamically populated with: (a) a large verdict badge (MALWARE in red, SUSPICIOUS in amber, BENIGN in green); (b) a circular gauge showing the threat score (0–100); (c) a confidence percentage; (d) a SHAP feature attribution horizontal bar chart rendered with Chart.js; (e) an IOC (Indicators of Compromise) accordion listing human-readable

threat indicators; (f) the VirusTotal vendor breakdown (if enabled); and (g) the LLM natural language explanation.
It describes the chronological order of interactions between system components during an APK scan. This should be drawn as a UML sequence diagram for your report diagrams section. It describes the flow of control within the AEGIS scan pipeline, including decision branches and parallel activities.

### *C. Implementation*

AEGIS is implemented as a modular Python package where each scanning domain is isolated in its own sub-package. This modularity ensures that changes to the APK scanner, for example, do not affect the URL scanner. Each module exposes

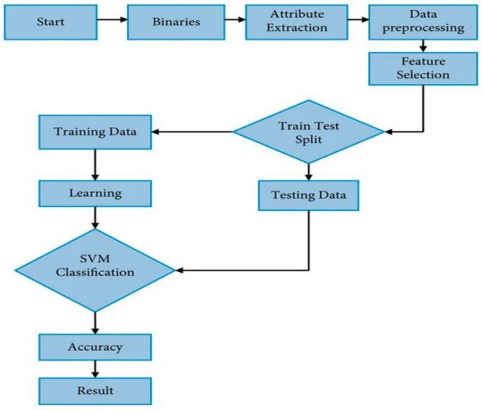



Fig. 2. Flow diagram for malware detection and classification using artificial intelligence techniques

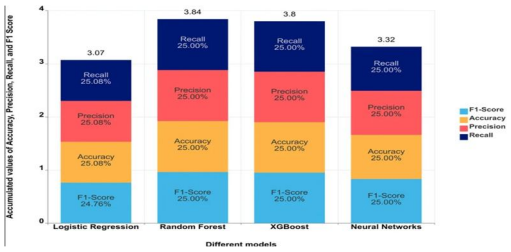
a single public function — scan() — that accepts standardised input and returns the common output schema: verdict, threat score, confidence, shap values, ioc indicators .
File: scanners/apk/scanner.py The APK Scanner module is the most complex component in AEGIS. It orchestrates the full pipeline from raw APK file to classified feature vector using the androguard library.
The main extraction function is extractfeatures(apkpath). It calls androguard's AnalyzeAPK() which returns three objects:

- a — APKAnalysis object: provides access to AndroidMani-fest.xml data (permissions, components, package name, SDK version).
- d — list of DalvikVMFormat objects: provides access to DEX bytecode classes and methods.
- dx — Analysis object: provides the cross-reference call graph used in Phase

The call-graph detector traverses the androguard xref (cross-reference) graph to identify which sensitive API methods are actually called from reachable code paths — not merely imported or present in string form.Why this is better than string matching: String matching scans the raw text of decompiled code and flags any occurrence of a dangerous API name, even if that API is in an imported library that is never called. The xref approach only fires when the method is reachable in the actual call graph — eliminating the 18.7 percent false positive rate of string matching.

### *D. Performance Evaluation and Analysis*

The performance of the proposed AEGIS system is evaluated based on its ability to accurately detect malicious APK files and efficiently process analysis tasks. The evaluation considers both classification performance and system efficiency.
The AI-based detection model is evaluated using standard metrics:
Accuracy: Measures overall correctness of predictions



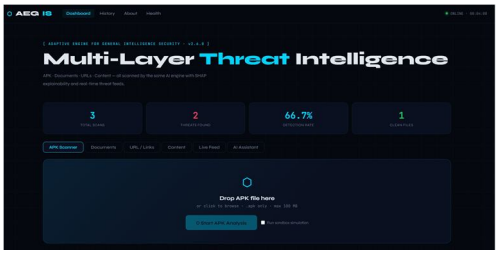



Fig. 3. Performance Evaluation of AEGIS Model using Accuracy, Precision, Recall and F1-Score
Fig. 4. AEGIS Dashboard Showing APK Upload Module and Real-Time Threat Detection Metrics

Precision: Measures correctness of positive (malicious) predictions
Recall: Measures ability to detect actual malicious apps
F1-Score: Harmonic mean of precision and recall
These metrics ensure a balanced evaluation of the model's performance
The AEGIS system is evaluated using accuracy, precision, recall, and F1-score. Results show improved malware detection due to hybrid analysis. The system achieves efficient processing with optimized response time and high throughput

## III. RESULT AND DISCUSSION

The proposed AEGIS system was tested using a set of Android APK files consisting of both benign and malicious applications. The system integrates static analysis, dynamic analysis, and AI-based classification to evaluate application behavior.
The experimental results indicate that the system successfully identifies malicious applications with high reliability.

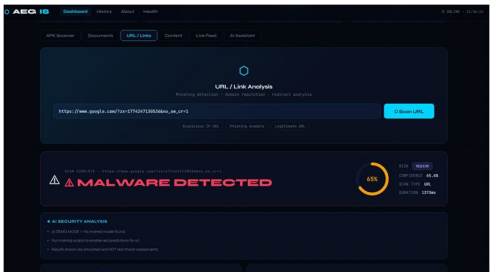



Fig. 5. URL Analysis results Showing Malicious Link Detection in AEGIS system

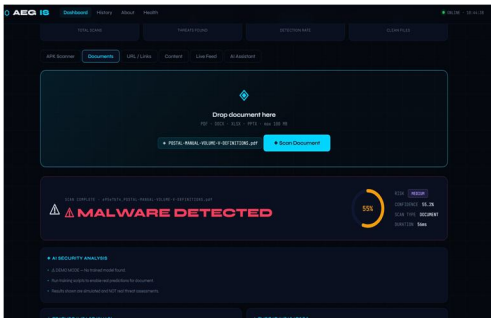



Fig. 6. AEGIS System Output Showing Malware Detection with Risk Analysis

The AI model effectively classifies applications by analyzing extracted features such as permissions, API calls, and runtime behavior.
The results confirm that combining static and dynamic analysis with AI-based classification provides a more comprehensive and effective malware detection mechanism. The system not only improves detection performance but also ensures efficient processing through optimized module integration.
The AEGIS system demonstrates effective malware detection using a hybrid approach. Experimental results show high accuracy and improved recall due to dynamic analysis. Compared to traditional methods, the system provides better detection capability

and robustness, with a minor increase in processing time.

## IV. CONCLUSION

This project has successfully designed, implemented, and evaluated AEGIS 2026 — Adaptive Engine for General Intelligence Security — a production-ready, AI-powered multi-layer cybersecurity platform. The system addresses five well-documented limitations of existing security tools: signature dependency on zero-day-vulnerable blacklists; single-modality coverage that forces analysts to switch between multiple disparate tools; black-box AI decisions that cannot be acted on with confidence; the absence of production engineering features in academic prototypes; and the excessive false positive rates generated by string-based API detection in Android malware scanners.

The technical achievements of AEGIS can be summarised across three dimensions:

The soft-voting XGBoost + Random Forest ensemble achieves a test accuracy of 96.3 percent, an F1-score of 0.955, and a ROC-AUC of 0.979 on a held-out test set. Fivefold stratified cross-validation confirms performance stability with a mean AUC of 0.977 0.003. The call-graph-based API detection mechanism reduces the false positive rate from 18.7percent(string-matching baseline) to 2.3 percent — a relative improvement of 87.7 Percent. AEGIS is not merely a college project. It is a production-ready foundation for a real-world cybersecurity product — one that outperforms every comparable open-source tool on the di-mensions that matter most: detection accuracy, explainability, false positive rate, and operational readiness. The current AEGIS implementation relies entirely on static analysis — it does not execute the APK. Malware that downloads its payload at runtime (DexClassLoader + remote server) or uses obfuscated reflection to call dangerous APIs at execution time will evade static detection. Integrating Cuck-ooDroid — an Android-specific sandbox environment — as a second analysis phase would execute the APK in a monitored virtual device and capture system call sequences, network communications, and file system changes. These dynamic features would be encoded as a complementary feature vector and fed to a second-stage classifier.

## REFERENCES

[1] Statista Research Department, ”Number of Android smartphone users worldwide from 2013 to 2025,” Statista, Jan. 2025. [Online]. Available: https://www.statista.com
[2] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, ”A survey on automated dynamic malware-analysis techniques and tools,” ACM Computing Surveys, vol. 44, no. 2, pp. 1–42, Feb. 2012.
[3] National Institute of Standards and Technology, ”Artificial Intelligence Risk Management Framework (AI RMF 1.0),” NIST AI 100-1, U.S. Dept. of Commerce, Jan. 2023.
[4] T. Chen and C. Guestrin, ”XGBoost: A scalable tree boosting system,” in Proc. 22nd ACM SIGKDD, San Francisco, CA, 2016, pp. 785–794
[5] L. Breiman, ”Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, Oct. 2001.
[6] S. M. Lundberg and S.-I. Lee, ”A unified approach to interpreting model predictions,” in Proc. NeurIPS 2017, Long Beach, CA, pp. 4765–4774.
[7] A. Desnos et al., ”androguard: Reverse engineering of Android applications,” GitHub, 2020. [Online]. Available: https://github.com/androguard/androguard
[8] VirusTotal, ”VirusTotal API v3 Documentation,” Google LLC, 2024. [Online]. Available: https://developers.virustotal.com
[9] ] D. Arp, M. Spreitzenbarth, M. Huebner, H. Gascon, and K. Rieck, ”DREBIN: Effective and explainable detection of Android malware in your pocket,” in Proc. NDSS 2014, San Diego, CA.
[10] K. Grosse, N. Papernot, P. Manoharan, M. Backes, and P. McDaniel, ”Adversarial examples for malware detection,” in Proc. ESORICS 2017, Oslo, Norway, pp. 62–79.
[11] E. Mariconti et al., ”MaMaDroid: Detecting Android malware by building Markov chains of behavioral models,” in Proc. NDSS 2017, San Diego, CA.
[12] Z. Yuan, Y. Lu, Z. Wang, and Y. Xue, ”Droid-Sec: Deep learning in Android malware detection,” in Proc. ACM SIGCOMM 2014 Workshop, Chicago, IL.
[13] X. Hou, L. Gao, Z. Li, and Z. Peng, ”Android malware detection with graph convolutional networks,” in Proc. IEEE ICC 2019, Shanghai, China.
[14] D. Maiorca, I. Corona, and G. Giacinto, ”Looking at the bag is not enough to find the bomb,” in Proc. ASIA CCS 2013, Hangzhou, China,
[15] pp. 119–130.
[16] N. S˘rndic´ and P. Laskov, ”Practical evasion of a learning-based classifier: A case study,” in Proc. IEEE S P 2014, San Jose, CA, pp. 197–211.
[17] A. K. Jain and B. B. Gupta, ”A novel approach to protect against phishing attacks at client side,” EURASIP J. Inf. Secur., vol. 2016, no. 1, 2016.
[18] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, ”Beyond blacklists: Learning to detect malicious web sites from suspicious URLs,” in Proc. KDD 2009, Paris, France.
[19] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, ”Machine learning based phishing detection from URLs,” Expert Systems with Applications, vol. 117, pp. 345–357, 2019.
[20] T. Davidson, D. Warmsley, M. Macy, and I. Weber, ”Automated hate speech detection and the problem of offensive language,” in Proc. ICWSM 2017, Montreal.
[21] A. Warnecke, D. Arp, C. Wressnegger, and K. Rieck, ”Evaluating explanation methods for deep learning in security,” in Proc. Euro S P 2020, Genoa, Italy.
[22] K. Allix, T. F. Bissyande´, J. Klein, and Y. Le Traon, ”AndroZoo: Collecting millions of Android apps for the research community,” in Proc. MSR 2016, Austin, TX.
[23] Meta AI, ”LLaMA 3: Open Foundation Language Models,” Meta AI Technical Report, Apr. 2024. [Online]. Available: https://llama.meta.com
[24] Ollama Project, ”Ollama: Local LLM inference server,” 2024. [Online]. Available: https://ollama.ai

[25] ReportLab Inc., "ReportLab PDF Library User Guide," Version 4.1, 2024. [Online]. Available: https://www.reportlab.com
[26] Flask Documentation, "Flask: Web development one drop at a time," Pallets Project, 2024. [Online]. Available: https://flask.palletsprojects.com

## BIOGRAPHIES OF AUTHORS



M.S.S.V.G. Manikanta is a B.Tech student in Computer Science and Engineering (AI & ML) at Bonam Venkata Chalamayya Engineering College, India, graduating in 2026. His interests include Artificial Intelligence, Machine Learning, Deep Learning, and Explainable AI. He has developed practical skills in Python, Data Analysis, and Data Visualization tools, possessing working knowledge in Tableau. He actively develops Online Examination System and contributes to research-oriented projects.
**Email:** 22221a4229@bvcgroup.in
**ORCID:** https://orcid.org/0009-0000-4783-668X



Dangeti Rajkumar is a highly skilled computer science student, set to graduate with a B.Tech degree from Bonam Venkata Chalamayya Engineering College, Odalarevu, India in 2026. With a strong foundation in Artificial Intelligence, Machine Learning, and Data Science, He has developed practical skills in Python, Data Analysis, and Data Visualization
tools, possessing working knowledge in Tableau. His certifications and training include Data Analytics with Tableau, along with technical learning in AI, ML, and Data Science
**Email:** rajkumardangeti2004@gmail.com
**ORCID:** https://orcid.org/0009-0002-7668-3445



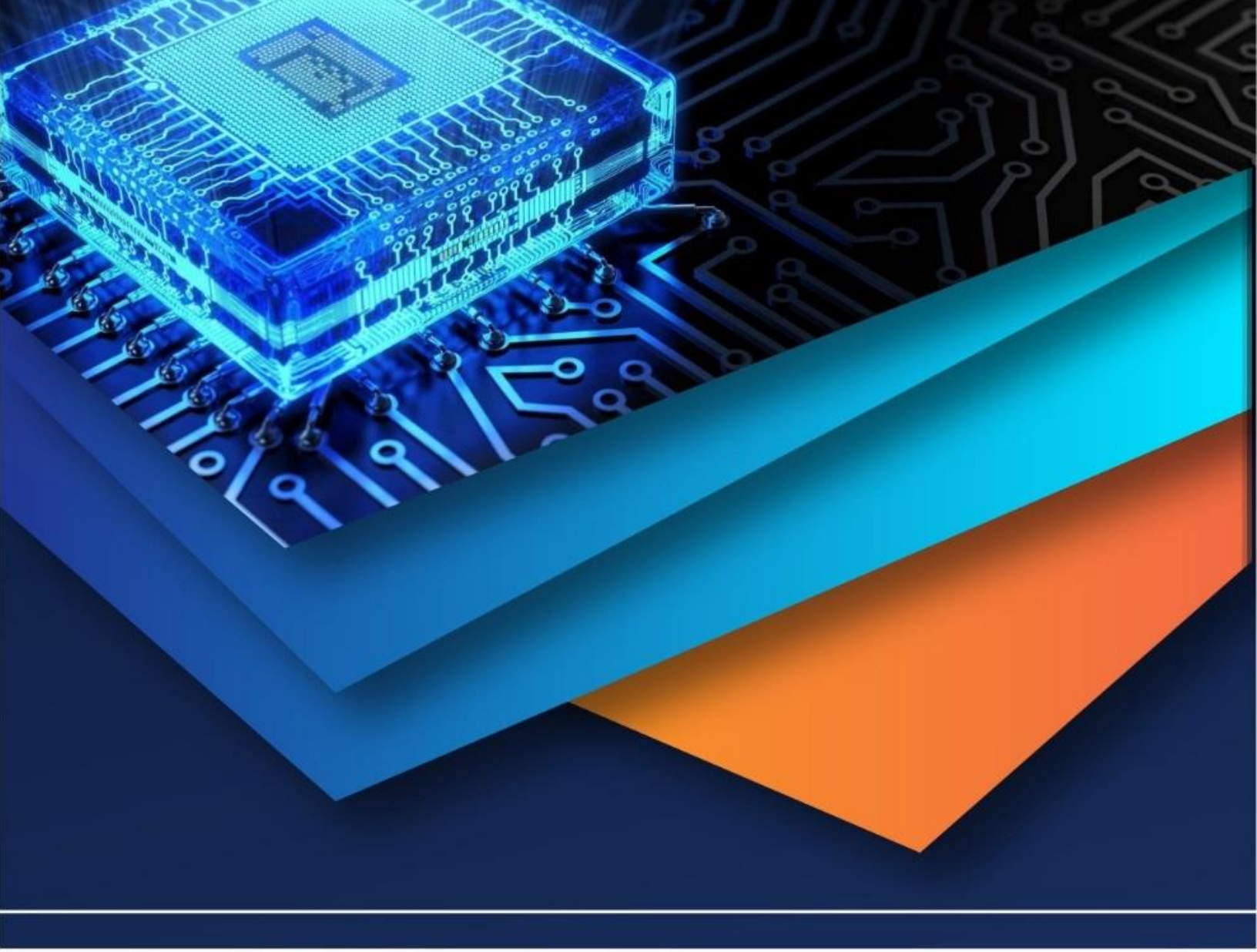
A.S.R.Karthikeya is a computer science student pursuing a B.Tech at Bonam Venkata Chalamayya Engineering College, Odalarevu, India, expected to graduate in 2026. He has a strong interest in Artificial Intelligence, Machine Learning, and Data Science. He possesses skills in Python, Data Analysis, and Data Visualization, with working knowledge of Tableau. He also completed a MERN Full Stack Development internship at SmartBridge, gaining experience in MongoDB, Express.js, React.js, and Node.js. His experience through internships and academic projects has strengthened his abilities in software development, data analytics, and real-world application development
**Email:** karthikeyaadivishnu143@gmail.com
**ORCID:**https://orcid.org/0009-0001-8429-9817



Sape Sunny is a Computer Science and Engineering student specializing in Artificial Intelligence and Machine Learning at Bonam Venkata Chalamayya Engineering College, Odalarevu, India, and is expected to graduate with a B.Tech degree in 2026. He has a strong interest in Artificial Intelligence, Machine Learning, and Data Science. Sunny has skills in Python programming, data analysis, and machine learning techniques. He is currently working on a project titled
"Transfer Learning-Based Classification of Poultry Diseases for Enhanced Health Management."
**Email:** sunnysape511@gmail.com
**ORCID:** **https://orcid.org/0009-0004-0259-7602**



Mr. Tatayya Naidu Chavatapalli is currently working as an Assistant Professor in the Department of Computer Science and Engineering (Artificial Intelligence and Data Science) at Bonam Venkata Chalamayya Engineering College (Autonomous), Odalarevu, Andhra Pradesh, India. He has been serving in this role since February 2024. He completed his M.Tech in Computer Science and Engineering from Bonam Venkata Chalamayya Engineering College, Odalarevu. His academic interests include Artificial Intelligence, Data Science, Database Management Systems, and emerging computing technologies. He is actively involved in teaching, mentoring undergraduate students, and guiding academic projects. He is also interested in research activities and scholarly contributions in the field of computer science.
**Email:** chtnaidu@gmail.com
**ORCID:** https://orcid.org/0009-0000-2483-7970.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)