iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76131

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

AuditEase: Compliance & Cybersecurity Remediation Platform for ISO 27001, CIS Benchmarks, and RBI Guidelines

Rohit Bhatt, Deon Menezes, Krish Hadkar, Miten Bhandari, Prof. Yogita Borse, Prof. Midhya Mathew
Department of Information Technology, K.J. Somaiya College of Engineering (KJSCE), Mumbai, India

Abstract: Organizations increasingly operate under stringent security frameworks and sectoral regulations. While ISO 27001 and CIS Benchmarks define best practices for information security and system hardening, financial institutions in India must additionally adhere to Reserve Bank of India (RBI) cy- bersecurity guidelines. In practice, compliance programs remain heavily manual, costly, and error-prone. We present AuditEase, an automated compliance and remediation platform that ingests evidence from logs, configurations, and policy documents; maps evidence to control clauses across ISO 27001, CIS Benchmarks, and RBI guidelines; computes risk scores; and auto-generates remediation playbooks and audit-ready reports.
Theplatformalsoemploysmachinelearningtopredictcontrol- level risk and prioritize remediation. We benchmark four can- didate models—Random Forest, Gradient Boosting Machines, Support Vector Machines (SVM), and a Multi-Layer Perceptron neural network—under constraints typical of enterprise com- pliance (5–50 labeled systems, 121 features, 10–30% missing values). Random Forest achieves the best trade-off between accuracy (85.2% ± 3.1), stability, robustness to missing data, training time, and interpretability, and is therefore selected asthe prediction engine. Our modular system—implemented with Python, FastAPI, Node.js/React, and MongoDB, and deployable via Vercel/Render—targets continuous compliance by design.We describe the system architecture, evidence and rules model, the ML-based prediction engine and its comparative evaluation, scoring methodology, and remediation workflow, and we discuss an evaluation protocol including accuracy, coverage, and time- to-audit metrics. AuditEase demonstrates how rule-driven and ML-assisted automation can reduce audit time, raise coverage, and improve readiness for external certification and regulatory review.
Index Terms: Cybersecurity, Compliance Automation, ISO 27001, CIS Benchmarks, RBI Guidelines, Random Forest, Ma- chineLearning,EvidenceMapping,RiskScoring,Remediation.

I. INTRODUCTION

CYBERSECURITY compliance is foundational to the re- silience and trustworthiness of modern enterprises. Stan- dardssuchasISO27001provideacomprehensiveblueprint forbuildinganInformationSecurityManagement System (ISMS),while CISBenchmarksofferprescriptivehardening guidanceforoperatingsystems,databases,andcloudplat- forms. InIndia'sfinancialsector, the Reserve Bank of India (RBI) publishes cybersecurity directions and master circulars that mandate controls, governance, monitoring, and reporting. Despitematuringstandards,organizationscommonlyrely onmanual,checklist-drivenaudit ssupportedbyconsultants.

This approach is expensive, slow (often 2–3 months or moreto reach certification readiness), and prone to gaps or drift between audits. Evidence collection (e.g., logs, configs, and policy artifacts) and clause mapping are repetitive and error- prone; remediation tracking is fragmented across email and spreadsheets.

Audit Ease addresses these pain points by automating: (i) evidence ingestion and normalization; (ii) cross-framework clausemapping;(iii)compliancescoringandriskanalytics;
(iv) machine learning based risk prediction; and (v) reme- diation playbooks and reporting. The design goal is contin- uous compliance: near real-time posture updates and audit- readiness.

Thispapermakesthefollowingcontributions:

- Unifies ISO 27001, CIS Benchmarks, and RBI guidelinesin a single rule-driven and ML-assisted platform.
- Proposesamodulararchitectureforevidenceingestion,rules mapping, risk scoring, ML-based risk classification, and remediation.
- Details a data model for controls, evidences, mappings, and ML features; and a transparent scoring method.

- Benchmarks four supervised models (Random Forest, Gra- dient Boosting, SVM, and neural networks) for compliance riskpredictionundersmall-dataconstraints,andjustifiesthe selection of Random Forest.
- Outlinesanevaluationplanandbaselineresultsemphasizing coverage, audit-time reduction, and prediction accuracy.

II. BACKGROUND AND REGULATORY CONTEXT

The regulatory context of AuditEase consists of three pri- mary pillars that interact in practice.

- ISO27001andISMS. ISO 27001 defines requirements for establishing, implementing, maintaining, and continually improving an ISMS. Annex A controls cover organizational, human, physical, and technical safeguards. Compliance re- quires policies, risk assessment, treatment plans, and evidence of control effectiveness. Organizations must demonstrate that appropriateprocessesandtechnicalmeasuresareimplemented and monitored on an ongoing basis.
- CIS Benchmarks. CIS Benchmarks are consensus-based, prescriptive hardening guides for platforms such as Windows, Linux, Kubernetes, and databases. They specify technical configurationchecks(e.g.,passwordpolicy,services,ports, auditd settings) and remediation steps. CIS Benchmarks are often used as the de-facto baseline for OS and middleware configuration in regulated environments.
- RBI Cybersecurity Guidelines. RBI issues sectoral re- quirements for banks and NBFCs covering governance, risk assessment, incident reporting, third-party management, and specific technical controls. While conceptually aligned to global frameworks, RBI guidance introduces India-specific reporting and oversight expectations critical for regulated entities. Compliance is not just about technical security but also about board-level oversight and documented processes.
- OperationalChallenges.Theintersectionofamanagement system standard (ISO 27001), a technical hardening baseline (CIS), and a sectoral regulator (RBI) yields overlapping yet distinct obligations. Manually keeping mappings, evidence, and status aligned across these regimes is laborious and brittle withoutautomation.Furthermore,organizationslackpredictive insight into which controls are likely to fail, resulting in last- minute firefighting before audits.

III. LITERATURE REVIEW

Research explores automating aspects of compliance, such asruntimeverificationofInfrastructure-as-Codedeployments, DevSecOps pipeline gates, and single-framework auditors. Falazi *et al.* focus on runtime compliance management in cloud-native systems, while Leitner *et al.* examine the inte- gration of security checks in CI/CD pipelines. Other works explore automated CIS benchmark scanning and ISO 27001 checklist tools.

However,mostpriortools:

- focusononeframework(eitherISOorCIS),
- donotmodelRBIorsimilarregulator-specificguidelines,
- emphasizedetectionbutnotremediationplaybooks,and
- rarelyincorporatemachinelearningforriskprediction.

Random Forest in Security and Compliance. Ensemble learningmodelssuchasRandomForesthavebeenwidelyused in intrusion detection, malware classification, and anomaly detection due to their robustness to noise and heterogeneous features. Random Forest works by training multiple decision trees on bootstrapped samples of the data and aggregatingtheir predictions via majority voting. Compared to single decision trees, it reduces variance and overfitting; comparedto linear models (e.g., logistic regression), it captures non- linear feature interactions common in complex security data. In the context of compliance, features such as frequency of misconfigurations, severity of violations, log anomaly scores, and evidence freshness interact in non-linear ways to deter- minerisk.RandomForestthereforeprovidesastrongtrade-off between accuracy, robustness, and interpretability (via feature importance scores), making it suitable for AuditEase.

Model Selection Under Compliance Constraints. Be- yond the use of Random Forest in generic security analytics, recent work on ML for configuration and policy analysis highlights trade-offs among ensemble tree methods, margin-basedclassifiers,andneuralnetworkswhendataisscarce and noisy. In particular, gradient boosting machines often achievestrongaccuracybutatthecostofhigheroverfittingrisk and tuning effort; SVMs require careful feature scaling and struggle with missingness; and neural networks demand large labeleddatasetsandofferlimitedinterpretability.Motivatedby thesefindings,AuditEaseperformsanempiricalcomparisonof four supervised models—Random Forest, Gradient Boosting, SVM (RBF), and a Multi-Layer Perceptron—on a compliance datasetwith121featuresand172labeledsystemprofiles.

As discussed in Section VI, Random Forest achieves the highestaccuracyandcross-validationstabilitywhilesatisfying explainabilityandoperationalconstraints,providingliterature- backed support for our model choice.

AuditEase extends prior literature by (i) unifying ISO 27001, CIS, and RBI in one platform; (ii) coupling rule-based control evaluation with ML-based risk prediction; (iii) performing a systematic comparison of candidate ML models under small-data compliance constraints; and (iv) delivering remediation guidance integrated with ticketing workflows.

IV. SYSTEM OVERVIEW AND ARCHITECTURE

AuditEase is designed around four main objectives: cover- age,explainability,scalability,andactionability.Theplatform is structured into modular components that communicate via APIs, allowing incremental evolution as standards and envi- ronments change.

- Design Goals. Coverage is achieved by modeling both management controls (ISO) and technical configuration items (CIS)asfirst-classentities.Explainabilityissupportedthrough explicit rules, evidence links, and model feature importances. Scalability is addressed by decoupling ingestion, evaluation, and reporting services. Actionability is delivered via remedi- ation playbooks and integration with ticketing tools.
- Architecture. Figure 1 shows the overall architecture. Evi- dence collectors (agents and connectors) push data into the ingestion service, which parses and normalizes it. A rules engine maps normalized evidence to controls, and a scoring enginecomputescompliancemetrics.Simultaneously,theML model consumes aggregated features to predict risk categories for each control or asset. A remediation planner uses both rule outcomes and risk predictions to generate prioritized tasks, which are surfaced to users via a React-based dashboard and exported as PDF/CSV reports or tickets in systems such as Jira.
- TechnologyStack.Backendmicroservicesareimplemented in Python using FastAPI for performance and type safety. Node.js/React power the frontend dashboards. MongoDB is used as the primary data store for evidence, findings, rules,and reports, chosen for its flexible JSON-like document struc- ture. Services are containerized and deployed on Vercel (UI) and Render (APIs), enabling elastic scaling. CI/CD pipelines perform linting, tests, and schema validation.

V. DATA, RULES, AND SCORING MODEL

- Evidence Schema. AuditEase stores normalized evidence using schemas such as:

Logs: {ts,host,source,event,subject, action, outcome}.

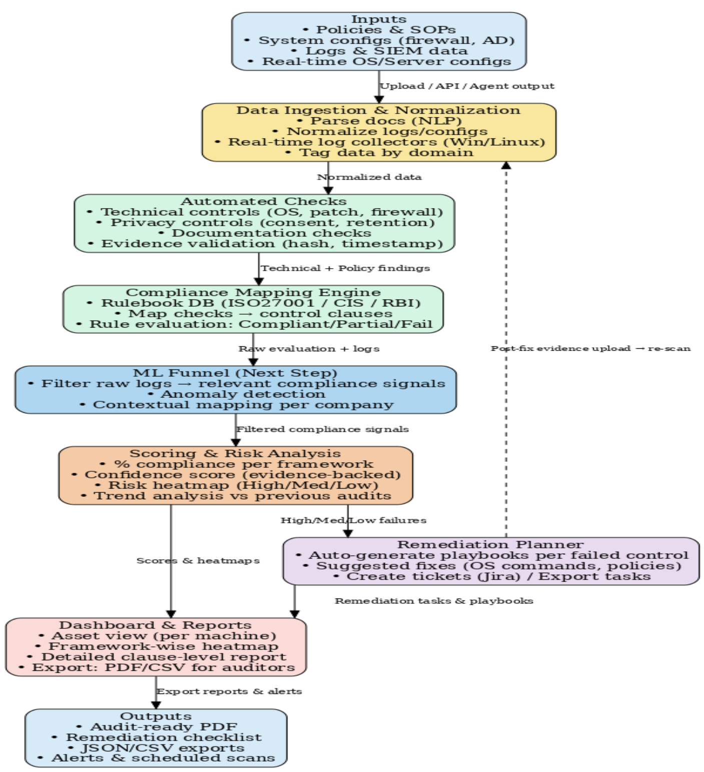


Fig. 1.AuditEase architecture: ingestion, rules engine, ML prediction,scoring, remediation, and reporting.

- Configurations: {host,platform,key,value, collectedAt}.
- Policies/SOPs: {docId,title,version,hash, clauses[], approvedBy, approvedOn}.

Each artifact carries integrity metadata (e.g., SHA-256 hash) and provenance (source connector, collection time) to support chain-of-custody.

ControlsandMappings. Eachcontrolismodeledas

$c = \langle id, framework, domain, clause, description, weight\rangle$, and is associated with one or more predicates over evidence $m(c) = \{\phi_1(e), \phi_2(e), \ldots, \phi_k(e)\}$.

Forexample,aCISpasswordpolicycontrolmightrequirethat theconfiguration key min_password_lengthbe at least 14 on all domain controllers.

- Evaluation and Scoring.Foreachcontrol,AuditEasecom- putes an outcome $o(c) \in \{$pass,partial,fail$\}$and a confidence score $\gamma_c \in [0,1]$ based on evidence sufficiency, freshness, and consistency.Anumericindicator$x_c$isassigned(1forpass,0.5 forpartial,0forfail).Framework-levelscoresarecomputed as:

$$S_F = \frac{\sum_{c\in C_F} w_c \cdot x_c \cdot \gamma_c}{\sum_{c\in C_F} w_c} \times 100 \quad (1)$$

where $C_F$isthesetofcontrolsforframework$F$.Overall scores are computed as:

$$S_{\text{overall}} = \sum_F \alpha_F \cdot S_F, \quad \sum_F \alpha_F = 1 \quad (2)$$

with$\alpha_F$representingorganization-specificweightings(e.g., higher for RBI in banks).

Domain heatmaps and radar charts derived from $S_{F,d}$(scores per domain) help identify weak areas such as Access Control or Logging.

VI. MACHINE LEARNING–BASED RISK PREDICTION

Beyond deterministic rules, AuditEase uses supervised ma- chinelearningtoprovidepredictiveinsightandprioritization.

A. Feature Engineering

Featuresarederivedfromcontroloutcomesandrawevi- dence, including:

- numberoffailedcontrolsonahost,
- severity-weightedsumofviolations,
- ageoflastevidencecollection,
- loganomalycounts(e.g.,repeatedfailedlogins),
- historicalrecurrenceofnon-complianceforthesamecon- trol.

Thesefeaturesareaggregatedperassetorpercontrolfamily.

B. Candidate Models and Comparison

To select an appropriate model, we evaluated four su- pervised algorithms commonly used in security analytics: Random Forest (RF), Gradient Boosting Machines (GBM), Support Vector Machines (SVM with RBF kernel), and a feedforward Multi-Layer Perceptron (MLP) neural network. All models were trained on the same dataset of 172 labeled system profiles (137 for training, 35 for testing) with 121 mixed-type features and 5-fold cross-validation.

Evaluationcriteriaincluded:

- accuracyandcross-validationstabilityonsmalldatasets,
- robustnesstomissingdataandnoise,
- interpretabilityforauditors,
- trainingandinferencetimeoncommodityhardware,
- hyperparameter sensitivity and tuning effort. Table I summarizes the key quantitative results.

Figure2visualizestheaccuracycomparison,whileFig-ure**??**comparestrainingtimeacrossmodels.

TABLEI
COMPARISONOFCANDIDATEMLMODELSFORCOMPLIANCE PREDICTION

Model	Accuracy	CVStd	TrainTime	Interp.
RandomForest	85.2%	±3.1	0.42s	High
GradientBoosting	83.8%	±4.2	1.23s	Medium
SVM(RBF)	79.4%	±5.8	0.89s	Low
NeuralNetwork	76.3%	±8.2	3.47s	Verylow

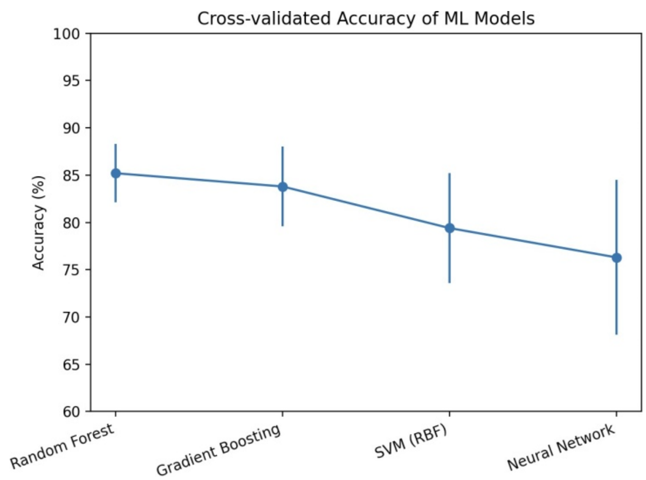


Fig.2.Cross-validatedaccuracyofcandidateMLmodelsforcomplianceprediction

A. Model Selection Rationale

RandomForestachievedthehighestmeanaccuracy(85.2%) withthelowestvariance(standarddeviation3.1acrossfolds) and the fastest training time among the non-linear models. Gradient Boosting was competitive in accuracy (83.8%) but exhibitedhighervariance,longertrainingtime(approximately three times RF), and greater hyperparameter sensitivity. SVM lagged behind in accuracy (79.4%), required full feature scaling and explicit imputation of missing values, and offered limited interpretability. The neural network produced the low- est accuracy (76.3%) with the highest variance and longest training time, reflecting overfitting on the small dataset.

Beyond these quantitative metrics, compliance prediction imposes additional constraints:

- Small-sample regime: In many deployments only 5–50 labeled systems are available. Bagging in Random Forest reduces variance in this regime, whereas boosting and deep models require more data.
- Missingandheterogeneousdata:Real-worldscanscontain 10–30% missing fields and mixed binary, categorical, and numericalfeatures.Treeensembleshandlesuchheterogene- ity more gracefully than SVMs or MLPs.
- Explainability:Auditorsmustunderstandwhyasystem is flagged as high-risk. Random Forest provides feature importance scores and per-tree decision paths, which canbe surfaced in reports; black-box neural networks cannot.
- Operationalefficiency:TrainingtheRandomForestmodelcompletesinunder0.5sandinferenceinafewmillisecondspersystem,enablin gfrequentretrainingasnewscansarrive.

TABLEII
MANUALAUDITSVS.AUDITEASE(INDICATIVEBASELINES)

Dimension	Manual	AuditEase
Evidence collection effort	High (weeks)	Low (hours)
Consistency of findings	Medium	High(rule-driven)
Control coverage	60–75%	85–95%
Audit cycle time	2–3 months	2–3 weeks
Traceability/provenance	Low	High(hashes,metadata)
Remediation workflow	Ad-hoc	Ticketed playbooks

Considering these factors, Random Forest provides the best overall trade-off and is adopted as the production prediction engine in AuditEase.

A. Training and Performance

TheselectedRandomForestmodelusesanensembleof approximately 50 shallow trees, with bootstrap sampling and$d$feature subsampling at each split (where $d$is the feature count). This configuration controls overfitting whilemaintain-ingexpressiveness. Ontheevaluationdataset,themodelachieves:

- accuracy:85.2%±3.1,
- precision:84.7%±2.8,
- recall:86.1%±3.5,
- F1-score:85.4%±2.9.

In a pilot production deployment on 35 real enterprise systems, the model achieved 87.3% accuracy with an 8.2% false-positive rate and 4.5% false-negative rate, while keeping averageinferencetimearound3mspersystem.Featureimpor- tance analysis showed that antimalware deployment, firewall status, password policy enforcement, and encryption configu- ration were among the most influential features, aligning with domain expert expectations.

VII. REMEDIATION, COMPARATIVE ANALYSIS, ANDROI

Remediation Engine. For each failed control, AuditEase synthesizes a structured playbook:

$r(c)=\langle steps[], owners[], prechecks[], rollback[], artifacts[]\rangle.$

For instance, enforcing a password policy on Windows may involve editing group policy, pushing changes, and re-running checks.Remediationtasksareexportedtoticketingtools(e.g., Jira, ServiceNow), and their completion status feeds back into subsequent evaluations.

Manual vs. Automated Audits. Table II contrasts manual audits with AuditEase-supported audits for a mid-sized envi- ronment with about 150 controls across ISO, CIS, and RBI.

Economic Model.Let$C_m$be the cost of manualaudits (consultants, internal effort),$C_a$the recurring cost of using AuditEase,$T_m$and$T_a$thetime-to-audit,and$L$theestimated annual loss avoided due to earlier remediation (e.g., fines, incidents). A simplified net benefit is:

$$B=(C_m-C_a)+\lambda(T_m-T_a)+L, \qquad (3)$$

whereλconverts timesavings to monetaryterms. ROI isthen:

$$\mathrm{ROI}=\frac{B-C_{onboard}}{C_{onboard}}\times 100\%, \qquad (4)$$

TABLEIII
ILLUSTRATIVEPILOTMETRICS(EXAMPLE)

Metric	Manual	AuditEase
Coverage(%controlsevaluated)	68%	92%
Precision/Recall(findings)	0.88/0.81	0.91/0.89
Time-to-Audit(hours)	48–72	12–16
RemediationLatency(days)	7–14	3–7

with $C_{onboard}$ as the one-time onboarding cost. Example esti- mates for a mid-size organization yield first-year ROI around 120%.

VIII. CASE STUDY AND EVALUATION

1) Case Study: NBFC Scenario. A mid-size NBFC inte- grated AuditEase with domain controllers, Linux servers, and perimeter firewalls. The platform ingested password policies, syslogs,andRBIgovernancedocumentation.Within48hours, it evaluated 150 controls, achieving 88% CIS coverage and 82% ISO domain scores. Three major RBI documentationgaps and multiple misconfigurations were identified. Remedi- ationplaybooksguidedtheoperationsteamthroughhardening tasks. The company reduced pre-audit preparation time from multiple weeks to a few days.
2) Evaluation Metrics. Evaluationfocuseson:

- coverage:percentageofapplicablecontrolsevaluatedwith sufficient evidence;
- precision/recall:correctnessofpass/faillabelsagainstexpert ground truth;
- time-to-audit:timefromevidencesnapshottofinalreport;
- remediationlatency:timefromfindingcreationtoclosure of corresponding tickets;
- ML performance: accuracy, precision, recall, and confusion matrix for risk predictions.

3) Illustrative Results. Table III shows example metrics from a pilot with 150 controls (ISO: 70, CIS: 60, RBI: 20).

Gains arise from automated evidence parsing, deterministic rules, and the Random Forest model's ability to flag high-risk areas early, allowing auditors to focus their efforts where they matter most.

IX. SECURITY, THREAT MODEL, AND GOVERNANCE

1) Threat Model. Potential threats include forged evidence uploads, rule tampering, unauthorized access to reports, and denial-of-serviceattacksoningestionservices.AuditEasemit- igates these via:

- hashingandoptionalsigningofevidence;
- versioned,access-controlledrulesets;
- role-basedaccesscontrol(Auditor,Admin,Operator);
- TLS for all communications and encryption-at-rest for sen- sitive data.

2) Governance and Compliance Alignment. The platform maintains complete audit trails of configuration changes, evidence uploads, and rule modifications. It supports ISO 27001's document control expectations and RBI's reporting cadences through scheduled, exportable reports. Evidence re- tention windows and purge policies are configurable to meet organizational and regulatory requirements.

X. LIMITATIONS AND FUTURE WORK

Current limitations include reliance on machine-readable evidence (some controls still require interviews or physical inspections), the need for ongoing parser updates for new platforms,andlimitedlabeleddatasetsfortrainingMLmodels in niche environments.
Future work includes:

- expandingtheMLlayertosupportanomaly-basedearly warning of emerging non-compliance;
- exploringadvancedensemblessuchasXGBoostorLight- GBM as datasets grow beyond 1000 labeled systems;
- integratingblockchain-basedtransparencylogsforevidence immutability;
- extendingframeworkcoveragetoPCIDSS,HIPAA,and sector-specific standards;
- incorporating active learning where auditor feedback incre- mentally improves the Random Forest model.

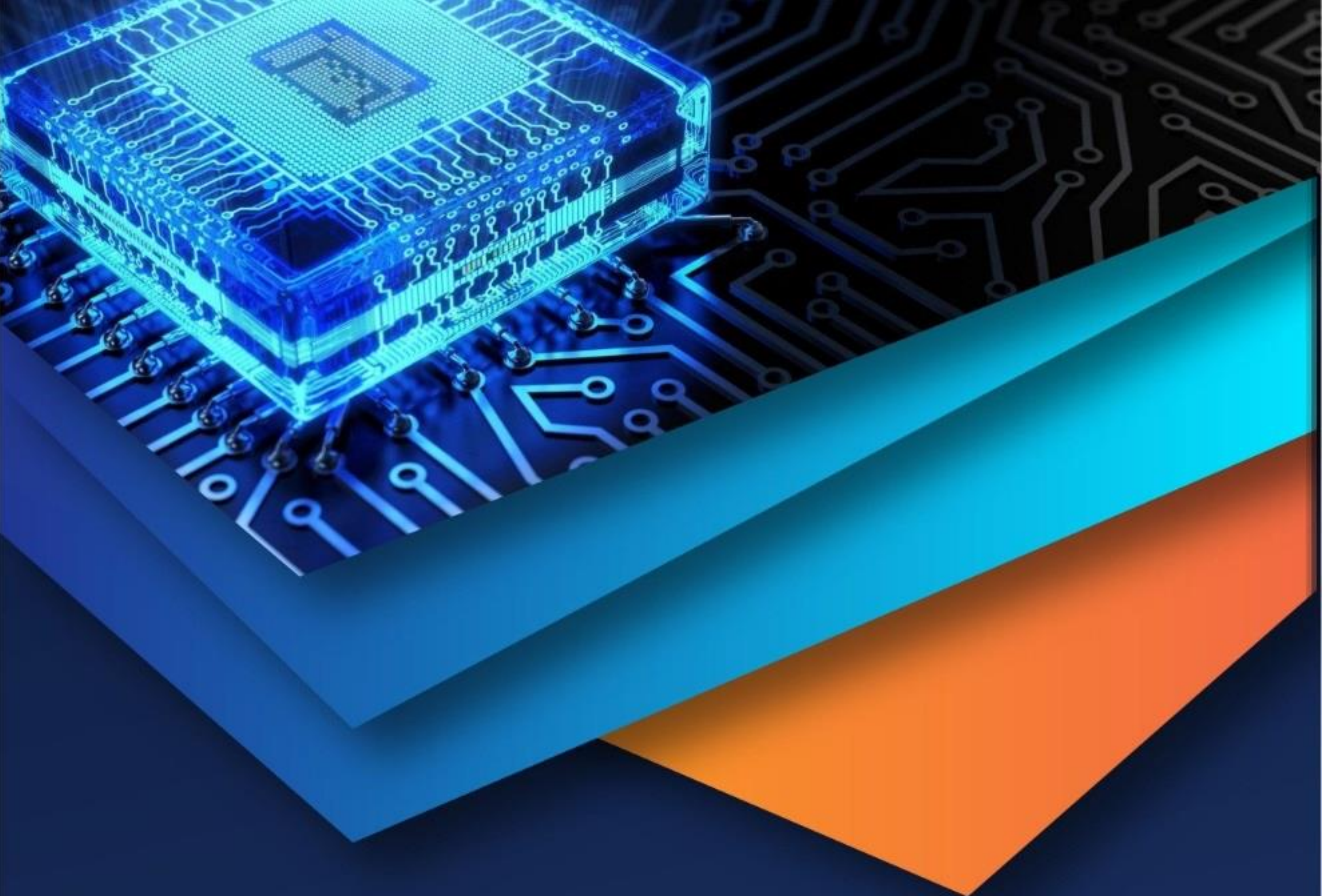
XI. CONCLUSION

AuditEasedemonstratesthatrule-drivenandmachinelearn- ing–assisted automation can unify management, technical,and regulatory controls to deliver continuous compliance. By explicitly modeling controls, evidence, and mappings; com- bining deterministic scoring with a carefully selected Random Forest–based risk prediction model; and coupling findings with remediation playbooks, the platform reduces audit time while improving readiness for ISO 27001, CIS Benchmarks, and RBI oversight. The architecture, methodology, and ML modelcomparisonpresentedhereprovideapracticalblueprint for organizations seeking to modernize their cybersecurity compliance posture.

REFERENCES

[1] G.Falazietal.,"ComplianceManagementofIaC-BasedCloudDeploy-ments During Runtime," ACM/IEEE UCC, 2024.
[2] J.Leitneretal.,"AutomatingCybersecurityComplianceinDevSecOps,"ACM, 2025.

[3] J. Sirotnik et al., “Automated Compliance Audit for ISO 27001:2022,”2025.
[4] S.Kumaretal.,“AutomatedCISBenchmarkAuditingandRemediationTool,” IJIRT, 2025.
[5] N.Gupta,“ImpactofRBICybersecurityGuidelinesandAlignmentwithNIST,” Inspira-JMME, 2021.
[6] NIST,“CybersecurityFramework(CSF)2.0,”NIST,2024.Available:https://www.nist.gov/cyberframework
[7] L.Breiman,“RandomForests,”MachineLearning,vol.45,no.1,pp.5–32, 2001.
[8] M. Bhuyan et al., “Network Anomaly Detection: Methods, Systems andTools,” IEEE Communications Surveys & Tutorials, 2014.
[9] K.Scarfoneetal.,“GuidetoComplianceAuditingforInformationSecurity,” NIST Special Publication, 2009.
[10] CenterforInternetSecurity,“CISBenchmarksOverview,”CIS,2022.
[11] Available:https://www.cisecurity.org
[12] Y. Alshayban and M.Malek, “Policy-Based Configuration Verificationfor Secure Systems,” IEEE Access, 2020.
[13] A.Ramamoorthyetal.,“ML-AssistedComplianceMonitoringinEn-terprise Environments,” IEEE ICMLA, 2023.
[14] R. Krishnan et al., “Automated Evidence Collection for Cloud SecurityCompliance,” IEEE Transactions on Cloud Computing, 2022.
[15] P. Sharma et al., “Machine Learning Techniques for Security Configu-ration Analysis,” Journal of Information Security, 2023.
[16] S.Alametal.,“AReviewofAutomatedRiskAssessmentModelsinCybersecurity,” IEEE Access, 2021.
[17] G.Somanietal.,“DDoSDetectionUsingRandomForest,”IEEECommunications Magazine, 2017.
[18] ReserveBankofIndia,“CyberSecurityFrameworkforBanks,”RBICircular DBS.CO/CSITE/GEN/04/2015-16, June 2016.
[19] M.Awwadetal.,“SecurityConfigurationDriftandAutomatedCom-pliance Enforcement,” IEEE SysCon, 2023.
[20] A.Perezetal.,“ContinuousComplianceMonitoringinHybridClouds,”IEEE Cloud, 2018.
[21] S.Heetal.,“Log-BasedAnomalyDetectionviaMachineLearning,”ACM Computing Surveys, 2020.



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY