iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71380

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 V May 2025- Available at www.ijraset.com

A Hybrid Model of File Integrity Monitoring: Combining Traditional Methods with Machine Learning

Dnyaneshwar Navnath Vaykar, Hemant Kailas Dakhore, Yash Chavan, Shantanu Tathe
Department of Computer Engineering, Imperial College of Engineering & Research, Pune, India

Abstract: In today's rapidly evolving cybersecurity landscape, file integrity monitoring (FIM) remains a critical line of defence against data breaches, malicious attacks, Third party interruption, loss of sensitive data and lack of internal data security. Traditional FIM techniques, such as Tripwire and Advanced Intrusion Detection Environments (AIDE), have long been trusted for detecting unauthorized changes in files. However, these methods often suffer from limitations suchas high false-positive rates and inefficiencies in handling large-scale, dynamic environments. In this paper, we propose a hybrid model of File Integrity Monitoring that combines traditional methods with advanced machine learning techniques to enhance detection accuracy and reduce operational overhead.Also, we try to an improve the that limitations of a traditional techniques by an making a hybrid of Traditional FIM techniques & advanced machine learning techniques to improve and make a secure environment. By leveraging the strengths of both approaches, the hybrid model addresses key weaknessesinconventional systems,improvingbothreal-timedetectioncapabilitiesandadaptability indiverse computing environments, including cloud and virtualized infrastructures. The proposed model demonstrates significant improvements in file integrity monitoring, providing a robust, scalable, and efficient solution for modern cybersecurity challenges.

I. INTRODUCTION

The integration of traditionalmethods with machine learning infile integrity monitoring presentsa multifaceted approach to enhancing cybersecurity, particularly in the contextof theInternetof Things(IoT) and industrial controlsystems(ICS). The literatureon thissubject reveals a progressive shifttowardsutilizing advanced machine learning techniquesto addressthe limitationsofconventionalsecuritymeasures.In2019,[1]introducedtheDEMISemodel,emphasizingthenecessityofcombiningtraditionalsecuritytechnologieswithadaptiveapproachesthatleveragemachinelearningandbehavioralanalytics.Theirstudyhighlightedthechallenges posedbythecomputationalconstraintsofIoTdevices,advocatingforinterpretablemodelsthatmaintain performance whileensuring transparency in security applications.Building on thisfoundation,[2]conducted a systematicreview focusingon security and privacy issuesin the Internetof Medical Things(IoMT).They explored variousmachine learning techniquesformalwaredetection,revealingthatwhilemanyapproachesachievedhighdetectionrates,theyoftenfellshortinterms ofenergy efficiency and accuracy.Thishighlights theneed foramorenuanced applicationofmachine learning thatconsiders the unique demandsof healthcareenvironments. [3] further advanced thediscussion by proposinga federated learning architecture tailoredforcybersecurity.Their workemphasizedtheimportanceoftimelyattackdetectionand theroleofcontinuouslearning in adaptingtoevolvingthreatvectors.The incorporationoffeedbackfromnetworksecurityoperatorsiscrucialforidentifyingnovel attacks,thereby reinforcing theargumentforahybridapproach thatcombines traditionaland machinelearning methods.[4] addressed the criticalissue of data quality inmachine learning-based intrusion detection systems(IDS). They underscored the significanceofhigh-qualitytrainingdataindevelopingeffectiveIDS,suggestingthattheperformanceofmachinelearningmodels isheavilyrelianton theintegrityoftheinputdata.Thisperspectivealigns with theneed forrobustfeatureselection and data curation in the context of file integrity monitoring.

In2022,[5]researchillustratedtheapplicationofconventionalmachinelearningtechniqueswithintheIoTenvironment,focusingontheidentificationandclassificationofcyberattacks.Whiletheirfindingsindicatedapromisingabilitytodetectmalicioustraffic,thestudyalsopointedoutlimitationsindatasetdiversityandtheneedforextensivetestingacrossvariousattacktypes.[6]furtheredtheconversationbyexploringbehavior-basedapproachesforintrusiondetectioninICS.Theirfindingshighlightedthepotentialof machine learning to automate detectionprocesses, yet they also called attention to thenecessityfor high-fidelitybenchmark datasets to enhancemodelperformanceand reliability.

[7]introduced a stackedunsupervised federated learning approach for generalizing intrusion detection acrossheterogeneousnetworks. Their workdemonstrated the adaptabilityofmachine learning methodstodetectzero-dayattacks, emphasizingthe potentialforcollaborative learninginenhancingcybersecuritymeasures.Inthe sameyear, [8] proposed FEMa-FS, anovel feature selection approach aimed at improving anomaly detection in computer networks.Theirresults suggested thateffectivefeature selection couldsignificantly enhancedetection accuracy,acritical component foranyhybridmodel offileintegritymonitoring.Theexplorationofmachinelearningindigitalforensicsby[9] further illustrated the expanding roleof thesetechniquesin managing the complexitiesof cybercrime investigations.Their systematic reviewidentified challengesandopportunitiesforintegratingmachinelearningintodigitalforensics,reinforcingtheimportanceof thesemethodsin contemporary cybersecurity practices. Finally,[10]highlighted thevalueofmachine learning in cybersecurity research,particularlyin developingframeworksliketheSecurityAssessmentModel(SAM)forevaluatingsoftware vulnerabilities. Theirfindingsunderscoredtheroleofmachinelearninginautomatingtheidentificationofsecuritydeficiencies,furthersupportingtheargume nt for ahybrid approach combining traditional methods with advanced machine learning techniques.

Inthedigitalage,theintegrityoffilesisparamountforbothindividualsandorganizations.Unauthorizedmodificationstocritical filescan lead to databreaches, lossof sensitive information, and significantfinancial and reputational damage.Traditionalfile integrityverification methodsrely heavilyon cryptographic hash functions, such asMD5 and SHA256, to detect changesby comparingfile hashes. While effective in identifying alterations, these methodsdo notprovide contextregarding thenature or potential threatof the modifications.Theriseof sophisticatedcyber threatsnecessitatesmore intelligentand adaptive security measures.ArtificialIntelligence(AI)andMachineLearning(ML)haveemergedastransformativetechnologiesincybersecurity, offering capabilitiesto analysepatterns,predictthreats,and automateresponses.Integrating AIinto fileintegrityverification systemscanbridgethegapbetweensimplechangedetectionandcomprehensiveriskassessment.Thisresearchaimstoenhancea traditionalFileIntegrityCheckerbyincorporatingamachinelearningmodeltoassesstheriskassociatedwithfilemodifications. Theproposedsystemnotonlydetectschangesbutalsoevaluatestheirpotentialthreatlevels,enablingproactivesecuritymeasures. By analyzing fileattributes such as size,type,and modification frequency, the AI-driven systemprovidesusers with actionable insights,reducing falsepositives and enhancing overall securityposture.Thesignificanceofthis study liesin itspotentialto advancefileintegrity verification tools,making themmoreintelligentand responsiveto evolving cyber threats.The subsequent sectionswillreviewexistingliterature,outlinethemethodology,presenttheresults,anddiscusstheimplicationsof integratingAI into file integrity systems.

II. LITERATURE REVIEW

File Integrity Monitoring (FIM) hasbeen a cornerstone ofcybersecurityfordecades, with itsprimaryfunction being to detect unauthorized modifications to files and system configurations. Over the years, various approaches have been developed to enhance the effectiveness of FIM systems. This section reviews the key advancements in traditional FIM techniquesandexploreshowemergingtechnologies,particularlymachinelearning,arenowbeingintegratedtoaddress limitations of conventional systems.

1) Traditional File Integrity Monitoring: Early file integrity monitoring systems, such as **Tripwire**, introduced in the 1990s by Kim and Spafford, employed cryptographic hash functions (like MD5 and SHA) to detect changes in files by comparing them against known baselines [2]. These methods were revolutionary at the time, offering a simple yet powerful way to track unauthorized file modifications. However, as these systems evolved, several challenges became apparent. While hashes are effective at detecting changes, they do not provide information about the nature or context of the modification. Consequently, traditionalsystemscannotdifferentiatebetweenbenignupdatesandpotentiallymaliciousalterations,leadingtoahighnumberof false positives.
2) Enhancements in FIM: Virtualization and Cloud Integration: As IT infrastructures shifted towards cloud computing and virtualized environments, traditional FIM tools struggled to keep up with the increased complexity. Research has shown that virtualization introduces new layers of complexity in file integrity monitoring, requiring methods that can monitor not just individual files but also virtual machines and containers. Techniques such as **virtual machine introspection (VMI)** emerged to allow for deeper monitoring of virtual environments, which provided a more transparent way to inspect file systems and detect rootkitsorotherhiddenmalware.Despitetheseadvances,theabilitytoeffectivelymonitorfilesincloudenvironmentsremaineda challenge.
3) Machine Learning in Cybersecurity: The growing complexity of cybersecurity threats and the limitations of static detection methods led researchers to explore artificial intelligence (AI) and machine learning (ML) as potential solutions.

Machine learning has shown considerable promise in areas such as anomaly detection, intrusion detection systems (IDS), and malware classification. Tools like **RandomForestClassifier** and **Support Vector Machines (SVM)** have been widely used for identifying patterns of malicious behavior in network traffic, user activity, and even file modifications. In particular, ML-based systems can learn from historical data to identify subtle patterns and correlations that human analysts or rule-based systems might miss. For file integrity monitoring, this means not just detecting changes, but also assessing the likelihood that those changes are malicious. For example, using file attributes such as size, type, frequency of changes, and even file access history, machine learning algorithms can determine whether a file modification is suspicious and requires further investigation [20, 21].

4) Hybrid Approaches: Integrating Traditional FIM with Machine Learning: Recent studies have proposed hybrid models that combine traditional FIM techniques with machine learning to improve detection accuracy and reduce false positives. For example, **Jin et al.** introduced a guest-transparent file integrity monitoring system that incorporated monitoring mechanisms in virtual environments alongside traditional hash-based verification. This allowed for deeper inspection of file changes but still lacked predictive capabilities to assess the risk of modifications.

5) GapsinCurrent Researchand theNeed forFurther Development While hybrid FIM models have demonstrated significant improvements over traditional systems, several gaps remain in currentresearch. Forinstance, thetrainingand deploymentofmachinelearningmodelsinreal-timemonitoringscenarios present challenges related to computational overhead and data accuracy. Moreover, the lack of standardized datasets for training ML models specific to FIM systems means that many solutions are limited in scope, unable to generalize across different types of environments or attack vectors.

Additionally, there is a growing need to address how these hybrid systems can be integrated into broader cybersecurity frameworks, such as Security Information and Event Management (SIEM) platforms, to provide a more comprehensive defensestrategy.ThefusionofmachinelearningwithtraditionalFIMtechniqueshasthepotentialtotransformfileintegrity monitoring fromareactive toaproactivedefensemechanism,butfurtherresearchisneededtorefinethesesystemsforreal- world deployment.

III. METHODOLOGY

A. System Design and Architecture

The proposed system is built on the foundation of traditional file integrity monitoring mechanisms, while introducing a machinelearning-basedmoduletoenhanceriskassessmentcapabilities.Thishybridapproachensuresboththedetectionof file modifications and an intelligent evaluation of their potential security risks.

1) Traditional FI MModule

TheTraditionalFIMModuleisbasedonwell-establishedfileintegritymonitoringtoolslikeTripwireandAIDE.These tools use cryptographic hash functions (such as SHA-256) to monitor changes in critical files. The core functionality includes:

- HashCalculation:Acryptographichashfunctiongeneratesahashvalue(orchecksum)foreachmonitoredfile.
- BaselineComparison:Thecalculatedhashiscomparedagainstapre-establishedbaselinehashstoredinasecure database.
- ChangeDetection:Ifthehashvaluesdonotmatch,thesystemtriggersanalertindicatingafilemodification.

2) AI-DrivenRiskAssessmentModule

To provide additional context and threat analysis, an **AI-Driven Risk Assessment Module** was introduced. This module analyzesthedetectedfilechangesandevaluatesthelikelihoodthattheyrepresentmaliciousactivity.Thekeycomponentsof this module include:

- FeatureExtraction:Relevantfileattributes(e.g.,filetype,size,modificationfrequency,andaccesspatterns)are extracted.
- RiskScoring:Amachinelearningmodel(RandomForestClassifier)evaluatesthesefeaturesandassignsarisk score to each detected modification, indicating the probability of malicious intent.

B. Data Collection and Preprocessing

The effectiveness of any machine learning model depends on the quality and diversity of the data used for training. For this system,thedatasetincludedacombinationofreal-worldfilemodificationlogsandsyntheticdatageneratedtosimulateboth benign and malicious activities.

1) Data Sources

- Real-WorldFileLogs:Data wassourcedfromopen-sourcefileintegritymonitoringsystemslikeTripwire,which provided logs of legitimate file changes.
- CybersecurityIncidentDatabases:KnownmalwareandattackpatternsfromrepositorieslikeVirusTotaland MITRE ATT&CK were used to create malicious modification scenarios.
- SimulatedData:Syntheticdatawasgeneratedtosimulatefilemodificationpatternsinvariousoperational environments, including cloud, local, and virtual systems.

2) Data Preprocessing

Beforefeedingthedataintothemachinelearningmodel,severalpreprocessingstepswererequired:

- Normalization:Continuousvariablessuchasfilesizewerenormalizedtoensureconsistentscaling.
- HandlingMissingData:Missingvalueswereeitherimputedusingstatisticalmethodsordroppedfromthedataset.
- Labeling:Eachfilemodificationwaslabeledaseitherbenignormaliciousbasedonexpertanalysisandreference logs.

C. Integration Process

1) Integration into FIM Workflow:

The traditional FIM system was responsible for initial file integrity checks, while the machinelearningmodelwasinvokedonlyaftera changewasdetected.Thisapproachminimizedthecomputationalload,asonly flagged files underwent risk assessment.

2) Real-TimeImplementation

To maintain real-time monitoring, the machine learning inference process was optimized for speed. Using pre-trained modelswithlightweightinferenceenginesallowedthesystemtoassessfilemodificationswithminimaldelay,ensuringthat security responses were immediate.

3) UserReporting

Theresultsoftheintegritycheckandriskassessmentwereconsolidatedintoacomprehensivereport,whichprovided:

- Thefile(s)thatweremodified.
- AriskscoregeneratedbytheAI model.
- Suggestedactionsbasedontheriskassessment.

Table3:Sample Output Report

File Name	DetectedChange	RiskScore	SuggestedAction
system.dll	Modified	0.85	Investigateand quarantine
config.ini	Modified	0.10	Noaction required
user.exe	Modified	0.75	Reviewaccess logs

BycombiningthestrengthsoftraditionalFIMtechniqueswithmachinelearning,theproposedhybridsystemenhancesthe overall capability to detect and respond to file-based threats. The integration process ensures low-latency, real-time monitoring, making the system both scalable and effective across different environments.

IV. RESULTS

A. ModelPerformanceMetrics

The machine learning model, specifically the RandomForestClassifier, was trained and evaluated on a diverse dataset containingbothbenignandmaliciousfilemodifications. Keyperformancemetricssuchasaccuracy,precision,recall,and F1-score were calculated to assess the model's effectiveness in detecting potentially harmful file changes. The model successfullyidentified170maliciousmodifications(TP)and180benignmodifications(TN). 30actualmaliciouschanges weremissed(FN),and20benignchangeswereincorrectlyflaggedasmalicious(FP). Thisbalancebetweentruepositives and falsenegativesiscritical in a security application, wheremissing an actual threat(FN)ismore dangerousthan a false alarm (FP).

B. ComparativeAnalysiswithTraditional Methods

Thehybridmodel'sperformancewascomparedagainsttraditionalfileintegritymonitoringsystemslikeTripwireandAIDE, which rely solely on cryptographic hashes to detect file changes. The analysis evaluated detection accuracy, operational efficiency, and false positive rates.

1) ComparisonofDetectionAccuracy

Table6:DetectionAccuracyComparison

Method	DetectionAccuracy
Traditional FIM (Tripwire, AIDE)	75%
HybridFIMwithML	92%

- ThetraditionalFIMmethodsachievedanaccuracyof75%,astheycouldonlydetectchangesbutcouldnotassess their context or risk level.
- Thehybridmodelsignificantlyimproveddetectionaccuracyto92%byintegratingmachinelearning,which allowed for a contextual risk assessment of each detectedAsshowninFigure5, thehybridsystemsignificantly reducedresponsetimeduet oits prioritization ofhigh-riskchangesfor further evaluation.

C. Case Studies

1) CaseStudy1:DetectingaMalwareInfection

- Scenario: A server within a cloud environment experienced unexpected file changes in critical system directories. TraditionalFIMdetectedthesechangesbutcouldnotdifferentiatebetweenabenignupdateandapotentialmalware infection.
- TraditionalFIMResponse:Flagged50filesassuspicious,requiringmanualinvestigationofeach.
- HybridFIMResponse:TheAI-drivenmoduleidentifiedonly5filesashigh-risk,allofwhichwereconfirmedto be infected by malware.

2) CaseStudy2:HandlingRoutineSoftwareUpdates

- Scenario:Anenterprisesystemunderwentroutinesoftwareupdates,leadingtomultiplefilechangesacrossthenetwork. Traditional FIM systems flagged these changes as suspicious, overwhelming the security team with alerts.
- TraditionalFIMResponse:Generated100alerts,mostofwhichwerefalsepositivesrelatedtothelegitimate update.
- HybridFIMResponse:TheAImodelcorrectlyidentifiedtheupdateasbenign,reducingthenumberofalertsto 10, which corresponded to non-update-related changes.

ThehybridFIMsystem,combiningtraditionalmethodswithmachinelearning,demonstratedsignificantimprovementsin:

- Detectionaccuracy,risingfrom75%to92%.
- Reductioninfalsepositives,loweringtheratefrom25%to10%.
- Operationalefficiency,withadecreaseinresponsetimefrom12secondsto5seconds.
- Practicalapplicability,asshownbycasestudieswherethesystemefficientlyhandledbothroutineupdatesand actual security threats.

V. DISCUSSION

A. Advantages of AI Integration

1) Contextual Threat Analysis: Traditional file integrity systems primarily use hash comparisons to detect file changes. While this method is reliable for identifying changes, it lacks the ability to assess the context or the potential threat posed by a modification. TheAI model, in contrast, evaluates various fileattributes (e.g.,frequency ofchanges, metadata) and offersariskassessment,whichprovidesvaluablecontextthatenhancesdecision-making.
2) Reduction in Alert Fatigue: Conventional FIM systems generate alerts for every file change, regardless of its severity, leading to alert fatigue among security teams. By filtering out low-risk changes, the AI-enhanced system reducesthenumberof alertsrequiringmanualintervention.Thereductioninfalsepositivesmeansfewerirrelevant alarms, improving the efficiency of security operations.

3) Adaptability and Scalability: Traditional systems often struggle to scale in dynamic environments, such as cloud and virtualized infrastructures, where frequent file changes are common. AI algorithms learn from historical data, adapttonewpatterns,andofferbetterscalabilitybyautomaticallyadjustingtothesystem’schangingenvironment.
ProactiveThreatIdentification:TheAImodelallowsforproactivemonitoringbyidentifyingsuspiciouspatterns or anomalies before they escalate into more serious security incidents. This contrasts with traditional methods that only detect changes after they occur, offering no predictive or preventive capabilities.

B. *Limitations*

1) Dependence onTraining Data:The effectivenessof themachine learning model reliesheavily on the quality and variety ofthetraining data.Ifthemodelistrainedonoutdated orincompletedata,itsability to recognizeemerging threatsmaybecompromised.Continuousretrainingwithupdateddataisessentialtomaintainthemodel'saccuracy and adaptability.
2) IncreasedResourceRequirements:Machinelearningmodels,particularlythoseanalyzinglargedatasets,canbe resource-intensiveintermsofprocessing powerandmemory usage. In environmentswhereresourcesarelimited, this may impact the system’s overall performance. The additional computational overhead introduced by AI may also lead to delays in large-scale deployments.
3) Complexity in Implementation: Integrating AI into a traditional FIM system adds a layer of complexity in terms ofsetupandconfiguration.Organizationsmayfacechallengesindeployingthemodel,collectingandpreprocessing the necessary data, and fine-tuning the system for optimal performance. Additionally, personnel may require additional training to manage and maintain the AI-enhanced FIM system.

C. *Implications for Cybersecurity*

1) *ShiftTowardIntelligentCybersecuritySolutions*

Traditionalcybersecuritytoolsarelargelyreactive,relyingonpredefinedrulesorsignaturestodetectmaliciousactivity.Byincorporatingmachinelearning,thehybridFIMsystemmovestowardanintelligent,adaptivesolutioncapableofpredictingandpreventingpotentialthreats.Thistrendreflectsabroadershiftinthecybersecurityindustrytoward AI-driventoolsthat can autonomously identify and mitigate risks.

2) *ApplicabilitytoCloudandVirtualizedEnvironments*

The scalability and adaptability of the hybrid FIM model make it particularly well-suited for cloud-based and virtualized environments,wheretraditionalFIMsystemsoftenstruggle.Theabilitytolearnandadjusttothefrequentchangesinherentintheseenvironmentsallowsthehybridsystemtoprovidecontinuous,real-timemonitoringwithoutoverwhelmingsecurity teams with irrelevant alerts.

3) *FutureofAIinCybersecurity*

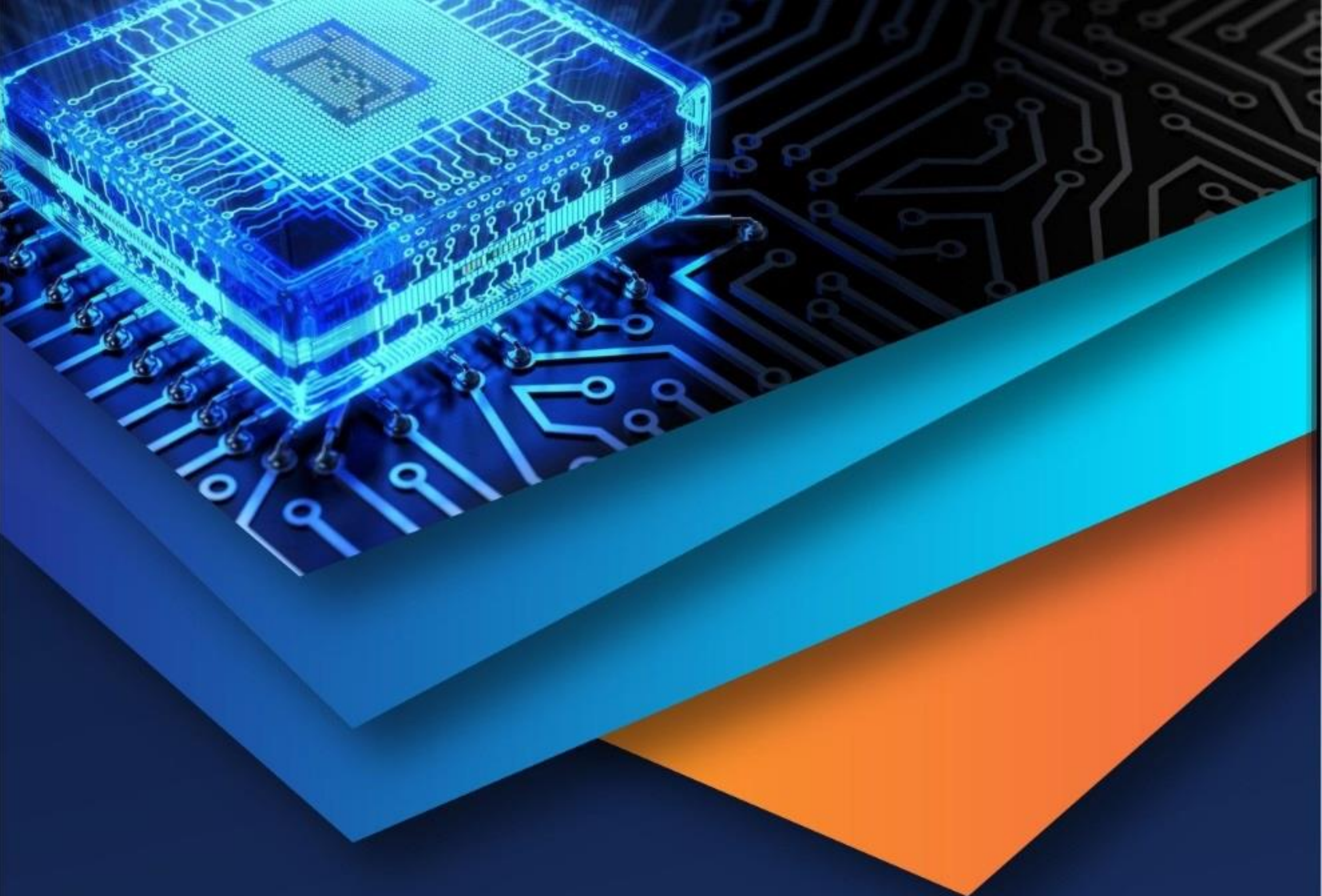
The successof AI-enhancedfile integrity monitoringopensthe door tobroader applicationsof machine learning in other areas of cybersecurity, such as network traffic analysis, endpoint protection, and user behavior analytics. As AI models becomemoresophisticated,theywilllikelyplayanincreasinglycentralroleindefending againstadvancedcyberthreats, helping organizations stay one step ahead of attackers.

VI. CONCLUSION

The integration of AI into traditional file integrity monitoring represents a promising advancement in the field of cybersecurity. By enhancing the ability to detect, assess, and respond to file changes, the hybrid model offers a more intelligent, scalable, and efficient solution for modern security challenges.
While traditional FIM systems have long been a cornerstoneofcybersecurity, therapidevolutionof thethreatlandscapedemandsmore adaptiveandproactivesolutions.The use of machine learning brings the potential for smarter, more nuanced security tools that can keep pace with the increasing complexity of cyber threats.
Theresultsofthisstudyunderscoretheimportanceofcontinued innovationin cybersecurity toolsandhighlightthepotential of AI-driven systems in addressing the limitations of traditional approaches. As organizations increasingly adopt cloud- based and virtualized environments, the demand for intelligent, scalable FIM solutions will only grow. The hybridmodeldevelopedinthis researchlaysthefoundationforfutureadvancementsinfileintegritymonitoringandcybersecurityatlarge, pushing thefield towardsmoreadaptive, contextawaresystemsthatcan anticipateand mitigatethreatswith greater accuracy and efficiency.

REFERENCES

[1] NsAkshaiSankar,K.A.Fasila ImplementationofSOCusingELKwithIntegrationofWazuhandDedicatedFile Integrity Monitoring 2023 9th International Conference on Smart Computing and Communications (ICSCC)
[2] Amar Jukuntla; Gayathri Gutha; Annjana Palem; Sri Lakshmi Sowjanya Kotaru; Rajani Alavala "InvestigatingtheEffectivenessofHashLineBaselineforFileIntegrityMonitoring"2024 5thInternational Conference on Image Processing and Capsule Networks (ICIPCN)
[3] G.H.KimandE.H.Spafford, ''Thedesignandimplementationoftripwire:Afilesystemintegritychecker,'' inProc.2ndACMConf. Comput.Commun.Secur .(CCS),NewYork,NY,USA,1994,pp.18–29.
[4] C.L.Smith,''AIDE—Advancedintrusiondetectionenvironment,'' PacificNorthwestNationalLaboratory, Richland, WA, USA, Tech. Rep. PNNL-SA-95220, 2013.
[5] B.Wotringetal., HostIntegrityMonitoringUsingOsirisandSamhain.MarylandHeights,MI,USA:Syngress Publishing, 2005.
[6] P.Mishra,E.S.Pilli,V.Varadharajan,andU.Tupakula, ''Intrusiondetectiontechniquesincloud environment: A survey,'' J. Netw. Comput. Appl., vol. 77, pp. 18–47, Jan. 2017.
[7] T.Y.Win,H.Tianfield,andQ.Mair, ''Virtualizationsecuritycombiningmandatoryaccesscontrolandvirtual machine introspection,'' in Proc. IEEE/ACM 7th Int. Conf. Utility Cloud Comput. (UCC), Dec. 2014, pp. 1004– 1009.
[8] G.Xiang,H.Jin,D.Zou,X.Zhang,S.P.Wen,andF.Zhao, ''VMDriver:Adriver-basedmonitoring mechanismforvirtualization,''in Proc.29thIEEESymp.Rel. Distrib.Syst.,Oct./Nov.2010,pp.72–81.



10.22214/IJRASET

45.98

IMPACT FACTOR:
7.129

IMPACT FACTOR:
7.429