International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

AI-Driven Threat Detection and Resilient Cloud Security Architecture for Modern Enterprise Systems

Dr. S. Jagadeesh Soundappan

Independent Researcher, USA

ABSTRACT: The rapid adoption of public cloud, hybrid cloud, multi-cloud, edge computing, containers, microservices, and software-defined infrastructure has transformed modern enterprise information systems while creating increasingly complex cybersecurity challenges. Mission-critical applications now operate across dynamic and geographically distributed environments in which conventional perimeter-based security mechanisms are insufficient to address sophisticated attacks, identity compromise, cloud misconfiguration, lateral movement, and previously unknown threats. Artificial intelligence (AI), machine learning (ML), deep learning (DL), behavioral analytics, threat intelligence, and automated security orchestration provide new capabilities for detecting abnormal activities and improving cyber resilience. This paper examines an AI-driven threat detection and resilient cloud security architecture designed for modern enterprise systems. The proposed architecture integrates continuous telemetry collection, intelligent anomaly detection, identity-centric zero-trust controls, threat intelligence, risk-based decision-making, automated response, and recovery mechanisms. A qualitative research methodology based on systematic literature analysis and conceptual architectural evaluation is adopted to investigate the effectiveness, scalability, adaptability, and trustworthiness of intelligent cloud defense. Recent research indicates that ML and DL can improve cloud intrusion detection, although dataset imbalance, limited datasets, computational cost, false positives, and evolving attacks remain important challenges. The study argues that AI should complement rather than replace conventional security controls and human expertise. A resilient architecture must combine intelligent detection with zero trust, defense-in-depth, secure configuration, continuous monitoring, automated containment, backup, recovery, governance, and human oversight.

KEYWORDS: Artificial Intelligence, Machine Learning, Cloud Cybersecurity, Threat Detection, Cloud Security Architecture, Cyber Resilience, Zero Trust, Anomaly Detection, Threat Intelligence, Security Automation, Enterprise Security, Multi-Cloud Security

I. INTRODUCTION

Cloud computing has become a fundamental component of modern enterprise information technology, enabling organizations to deploy applications and infrastructure with greater flexibility, scalability, availability, and cost efficiency. Enterprise systems increasingly use combinations of public cloud, private cloud, hybrid cloud, multi-cloud, edge computing, container platforms, microservices, serverless computing, and software-as-a-service applications. Although these technologies improve business agility, they also transform the cybersecurity environment. Data and workloads are no longer concentrated within a clearly defined organizational network, while users, applications, devices, APIs, and services may operate across different geographic locations and cloud providers. As a result, security architectures based primarily on network perimeters are becoming less suitable for protecting modern enterprise resources. NIST's Zero Trust Architecture emphasizes that organizations should not grant implicit trust to users or assets based merely on network location or ownership and should instead focus protection on users, assets, and resources. This architectural transformation is particularly important for enterprises operating critical applications because security failures can cause financial losses, operational disruption, regulatory consequences, reputational damage, and loss of customer confidence. Consequently, modern cloud cybersecurity requires an architecture capable of continuously observing, analyzing, protecting, and recovering enterprise resources across distributed environments.

Conventional security technologies such as firewalls, intrusion detection systems, antivirus software, endpoint protection, access-control mechanisms, encryption, and security information and event management platforms remain essential components of enterprise defense. However, the scale and complexity of modern cloud infrastructures make it

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

increasingly difficult for security teams to rely exclusively on static rules and manual analysis. Attackers can exploit stolen credentials, insecure APIs, vulnerable software dependencies, excessive privileges, exposed storage, compromised endpoints, and cloud configuration weaknesses without necessarily triggering conventional perimeter defenses. In addition, modern enterprises generate enormous volumes of telemetry from cloud platforms, identity providers, applications, network devices, containers, databases, endpoints, and infrastructure-management systems. Artificial intelligence provides an opportunity to transform this data into actionable security intelligence. ML algorithms can establish behavioral baselines and identify deviations, while deep-learning models can analyze complex relationships among multiple security events. Recent systematic research on cloud intrusion detection shows that ML and DL are increasingly used to address the limitations of conventional intrusion detection in dynamic cloud environments, although challenges involving datasets, imbalance, cost, and real-time adaptability remain. Therefore, AI-driven cybersecurity should be considered not simply as a new detection tool but as an intelligence capability embedded throughout the enterprise security architecture.

AI-driven threat detection can support a more proactive and adaptive approach to cybersecurity. Instead of treating security events independently, intelligent systems can correlate authentication events, network activity, application behavior, endpoint signals, cloud configuration changes, and threat-intelligence information to identify potentially coordinated attacks. For example, an AI system may recognize that an unusual login by a privileged account is followed by abnormal API activity, access to sensitive resources, and unexpected data transfers. Individually, these events may appear legitimate, but their combined context can indicate account compromise or malicious lateral movement. AI-based behavioral analytics can therefore help identify attack patterns that are difficult to recognize through static rules. The same intelligence can support risk-based access control by dynamically evaluating user identity, device posture, resource sensitivity, historical behavior, and current threat conditions. NIST's cloud-native zero-trust guidance recommends moving toward identity-centric policies involving application and service identities and technologies such as API gateways, sidecar proxies, and service meshes for enforcing granular controls across multi-cloud and hybrid environments. Integrating AI with zero trust can consequently enable continuous risk evaluation rather than relying on one-time authentication or assumptions about trusted internal networks.

Threat detection alone, however, does not guarantee cyber resilience. Modern enterprise systems must be capable of continuing essential operations during attacks and recovering rapidly when prevention mechanisms fail. Resilient cloud security therefore requires multiple coordinated layers encompassing prevention, detection, response, containment, recovery, and continuous learning. AI can contribute to each stage by prioritizing vulnerabilities, detecting abnormal activity, predicting attack progression, recommending containment actions, and learning from previous incidents. Nevertheless, AI introduces its own security and governance challenges. Models can produce false positives and false negatives, become less effective because of model drift, depend on incomplete or biased datasets, and potentially become targets of adversarial manipulation. Furthermore, highly automated security decisions may cause service disruption if the model incorrectly identifies legitimate activity as malicious. NIST's AI Risk Management Framework provides a structured approach for managing AI risks and promoting trustworthy and responsible AI throughout the lifecycle. Therefore, the objective of this research is to examine an AI-driven threat detection architecture that combines intelligent analytics with zero-trust access control, defense-in-depth, automated response, and recovery capabilities. The research focuses on developing a resilient security model in which AI improves visibility and decision-making while conventional controls and human oversight provide safeguards against errors and emerging AI-specific risks.

II. LITERATURE REVIEW

Existing literature demonstrates that cloud computing has changed the assumptions underlying conventional cybersecurity architectures. In traditional enterprise environments, organizations commonly relied on centralized networks, fixed infrastructure, and clearly defined boundaries between internal and external systems. Cloud computing has introduced dynamic resource allocation, distributed workloads, remote access, multi-cloud deployments, service APIs, containerized applications, and third-party dependencies. Consequently, security must increasingly protect individual resources rather than simply defend a network perimeter. NIST SP 800-207 establishes zero trust as an architectural approach in which trust is not automatically granted according to physical or network location. Authentication and authorization are treated as separate security functions that occur before access to enterprise resources. The cloud-native extension of this concept emphasizes application and service identities, granular policy enforcement, and security mechanisms that can operate consistently across on-premises and multiple cloud environments. This literature is important for AI-driven threat detection because intelligent security decisions require

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

contextual information about identities, resources, devices, and relationships. An AI system that identifies abnormal traffic without understanding the sensitivity of the affected resource may generate less useful results than a system that combines network behavior with identity, application, and asset context.

A substantial body of research investigates ML and DL for intrusion detection. Traditional signature-based systems are effective when attack patterns are known and clearly represented, but they can struggle with novel attacks and rapidly changing threat behavior. Anomaly-based detection addresses this limitation by learning representations of normal activity and identifying deviations. Supervised ML algorithms can classify known attack categories, while unsupervised and semi-supervised approaches can identify previously unknown patterns. Deep learning can analyze high-dimensional and sequential data, including network flows, logs, authentication events, and application telemetry. A 2025 systematic literature review of cloud intrusion detection reports that conventional intrusion detection and prevention systems have difficulty adapting to the dynamic nature of cloud environments and that ML/DL approaches have become increasingly important. However, the review identifies small datasets, imbalanced datasets, high computational costs, and the need for real-time adaptive systems as continuing challenges. Another 2025 systematic study of ML-based intrusion detection similarly highlights limitations in commonly used datasets, including outdated attack scenarios and class imbalance. These findings indicate that algorithm selection alone cannot determine the success of AI-driven security. Model quality depends strongly on representative data, appropriate evaluation metrics, continuous validation, and the ability to adapt to changing cloud environments.

Research has also expanded from isolated intrusion detection toward intelligent security operations and automated response. Enterprise security teams receive alerts from numerous sources, including endpoint protection, network monitoring, identity systems, cloud platforms, vulnerability scanners, application-security systems, and threat-intelligence feeds. The volume of these events can create alert fatigue and delay the investigation of genuinely dangerous incidents. AI can assist by correlating multiple events, identifying attack sequences, assigning risk scores, prioritizing alerts, and recommending response actions. When integrated with security orchestration and automated response platforms, AI can support actions such as disabling compromised credentials, terminating suspicious sessions, isolating workloads, blocking malicious network connections, or escalating incidents to human analysts. However, automation introduces a significant operational risk in mission-critical environments. An incorrect automated action can disrupt legitimate services, interrupt transactions, or isolate essential systems. Therefore, the literature and practical architecture principles support graduated automation in which high-confidence, low-impact actions may be automated while high-impact decisions require human authorization. Explainability is also important because security analysts must be able to investigate the reasoning behind an AI-generated alert or response. AI should consequently serve as a decision-support and automation capability within a controlled security-operations framework rather than operating as an unrestricted autonomous defender.

A further research direction concerns the security, privacy, and governance of AI itself. Security analytics may require access to sensitive logs containing user identities, customer information, application behavior, system configurations, and business activity. Centralizing this information for model training can increase privacy and data-governance risks. Distributed and privacy-preserving learning approaches can potentially reduce the need to transfer raw data between organizations or cloud environments. At the same time, AI systems can become targets for adversarial manipulation, including training-data poisoning, evasion, model exploitation, and malicious inputs. NIST's AI RMF emphasizes four core functions—govern, map, measure, and manage—and treats AI risk management as a continuous activity across the AI lifecycle. The current NIST AI RMF program is also being revised, while NIST released a concept note in April 2026 for a profile addressing trustworthy AI in critical infrastructure, demonstrating the growing importance of AI governance in high-impact environments. The literature therefore suggests that resilient cloud security requires more than accurate detection models. It requires trustworthy AI, reliable data, secure model pipelines, privacy protections, explainability, zero-trust access control, response governance, and continuous monitoring. A major research gap remains the integration of these elements into a unified architecture that addresses detection and resilience simultaneously. This study addresses that gap by conceptualizing AI as an intelligence layer within a broader cloud security and cyber-resilience architecture.

III. RESEARCH METHODOLOGY

This research adopts a qualitative, systematic, and conceptual methodology to examine AI-driven threat detection and resilient cloud security architecture for modern enterprise systems. The methodology is designed to identify established research findings, compare architectural approaches, determine technological advantages and limitations, and develop a

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

conceptual security architecture suitable for distributed enterprise environments. The primary research question is: How can AI-driven threat detection be integrated with resilient cloud security mechanisms to improve the protection of modern enterprise systems? Supporting questions investigate which AI techniques are most suitable for cloud threat detection, how zero-trust principles can complement intelligent analytics, how automated response can improve containment, how resilience can be maintained during successful attacks, and what governance mechanisms are required to ensure trustworthy AI deployment. The study uses peer-reviewed research articles, systematic reviews, recognized cybersecurity standards, government publications, and technical guidance as major evidence sources. Recent research on cloud intrusion detection is particularly relevant because it evaluates the use of ML and DL in environments characterized by dynamic workloads and rapidly changing infrastructure. NIST publications are used to establish architectural foundations for zero trust and AI risk management. This combination of academic and standards-based evidence supports a methodology that considers both technical performance and practical enterprise requirements.

The literature-selection process uses predefined inclusion and exclusion criteria. Publications are included when they directly address AI or ML-based cybersecurity, cloud threat detection, cloud intrusion detection, cyber resilience, zero trust, threat intelligence, security automation, or related enterprise-security architecture. Priority is given to peer-reviewed publications, systematic literature reviews, standards, and authoritative cybersecurity organizations. Recent publications are emphasized because cloud architectures and AI capabilities evolve rapidly, although foundational works are retained when they establish important concepts. Search terms include combinations such as “AI-driven cloud threat detection,” “machine learning cloud intrusion detection,” “resilient cloud cybersecurity,” “AI cybersecurity architecture,” “zero trust cloud security,” “AI-based anomaly detection,” “cloud security automation,” and “enterprise cyber resilience.” The collected literature is then organized into thematic categories: AI-based threat detection, behavioral analytics, identity security, zero trust, cloud infrastructure protection, application security, threat intelligence, automated response, recovery, privacy, explainability, adversarial AI, and AI governance. Studies that focus on unrelated AI applications or security problems without meaningful cloud or enterprise relevance are excluded from the primary analysis. The process aims to produce a structured evidence base that allows findings from different research streams to be compared and synthesized into a unified architectural model.

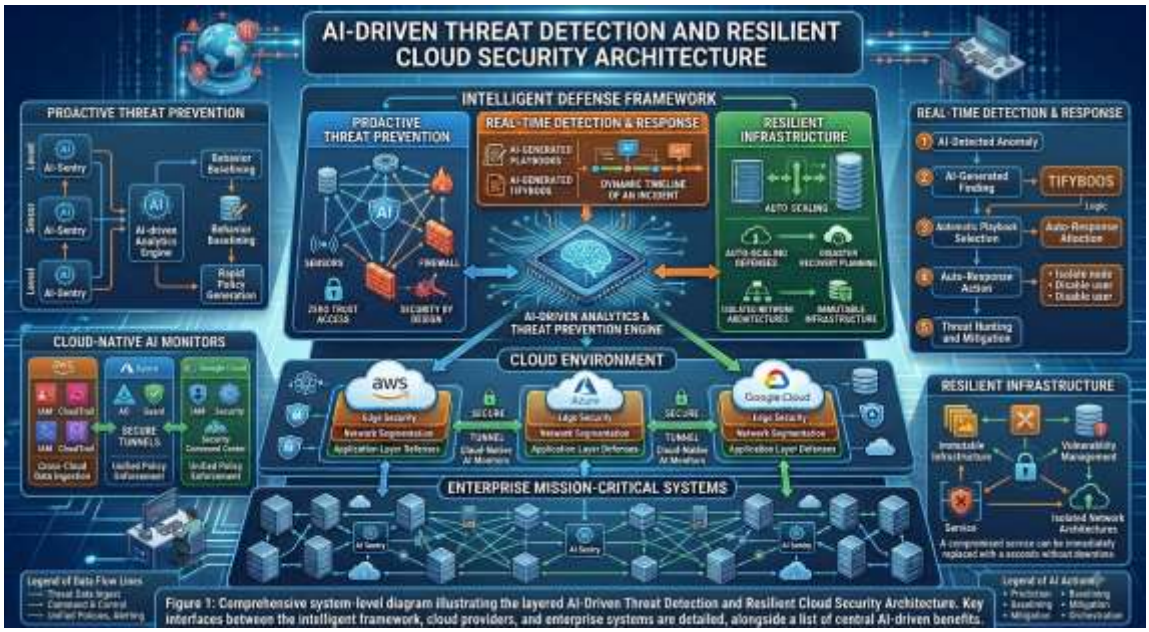


Fig1: AI-Driven Threat Detection and Resilient Cloud Security Architecture

The proposed architecture is evaluated using multiple qualitative and quantitative dimensions derived from the literature. The first dimension is threat-detection effectiveness, examining the ability of AI models to identify known, unknown, and evolving attacks. Where numerical results are available, precision, recall, F1-score, accuracy, false-positive rate, false-negative rate, and detection latency are considered. The second dimension is response effectiveness,

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

assessing whether intelligent analytics can reduce the time between initial compromise, detection, containment, and recovery. The third dimension is scalability, considering the ability to process telemetry across large numbers of users, devices, applications, containers, workloads, and cloud services. The fourth dimension is adaptability, examining whether models can respond to changing workloads, new attack techniques, software changes, and concept drift. The fifth dimension is resilience, assessing the ability of enterprise systems to maintain essential services and recover following security incidents. The sixth dimension is trustworthiness, incorporating explainability, robustness, privacy, transparency, governance, and human oversight. The seventh dimension is operational feasibility, including computational cost, data requirements, integration complexity, skills, maintenance, and compatibility with existing enterprise security platforms. These dimensions prevent the research from treating model accuracy as the only measure of cybersecurity effectiveness.

Based on the literature analysis, the research proposes a layered architecture containing eight interconnected components. Layer 1—Asset and Resource Discovery: continuously identifies applications, databases, workloads, identities, devices, APIs, cloud resources, and their dependencies. Layer 2—Security Telemetry: collects logs, network flows, authentication events, endpoint information, application traces, cloud-control-plane activity, and configuration changes. Layer 3—AI Analytics: applies supervised learning, unsupervised anomaly detection, behavioral modeling, deep learning, and risk scoring to identify suspicious activity. Layer 4—Context and Threat Intelligence: enriches detected events with asset criticality, identity information, vulnerability data, known indicators, attack techniques, and external intelligence. Layer 5—Zero-Trust Enforcement: continuously validates users, devices, applications, and services and applies least-privilege access policies. NIST's multi-cloud zero-trust model supports identity-based policies and application-level enforcement across distributed environments. Layer 6—Security Orchestration and Response: translates high-confidence AI findings into controlled actions such as authentication challenges, privilege reduction, session termination, network blocking, and workload isolation. Layer 7—Resilience and Recovery: provides backup, redundancy, disaster recovery, service restoration, and continuity mechanisms so that security incidents do not automatically become prolonged business failures. Layer 8—Governance and Continuous Learning: monitors model performance, investigates false positives and false negatives, evaluates model drift, validates AI decisions, and incorporates analyst feedback. Future empirical research can implement this architecture within a controlled multi-cloud test environment and compare AI-assisted defense against conventional security controls using representative attack scenarios. Evaluation should measure detection accuracy, detection latency, response time, service availability, recovery time, computational overhead, false-positive rates, and analyst workload. This methodology provides a practical foundation for testing whether intelligent threat detection can improve not only cybersecurity detection but also the broader resilience of enterprise cloud systems.

Advantages

Early threat detection: AI can identify suspicious behavior before attacks develop into major incidents.
Continuous monitoring: Intelligent systems can monitor cloud infrastructure, applications, identities, endpoints, and networks continuously.
Detection of unknown attacks: Behavioral and anomaly-detection models can identify deviations that do not match predefined signatures.
Large-scale data analysis: AI can process massive volumes of security telemetry more efficiently than manual analysis.
Improved alert prioritization: Machine learning can correlate events and prioritize high-risk incidents.
Faster incident response: AI-assisted orchestration can reduce the time required to contain high-confidence threats.
Adaptive security: Models can learn from changing behavior and emerging attack patterns when appropriately maintained.
Zero-trust enhancement: AI-based risk scoring can support context-aware authentication and authorization decisions.
Improved cloud visibility: Integrated telemetry can provide a more comprehensive view of distributed cloud resources.
Greater cyber resilience: Combining detection, containment, redundancy, backup, and recovery reduces the potential impact of successful attacks.
Reduced security-operations workload: AI can automate repetitive investigation and correlation tasks, allowing analysts to focus on complex incidents.
Predictive risk analysis: Historical and real-time information can support identification of vulnerabilities and emerging risks before exploitation.
Cross-environment protection: The architecture can be applied across hybrid-cloud and multi-cloud infrastructures rather than being restricted to a single network.
Continuous learning: Feedback from analysts and incident investigations can be used to improve future detection and response.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

Disadvantages

High implementation cost: AI-driven security requires investment in computing resources, software, data infrastructure, integration, and skilled personnel.

Dependence on data quality: Poor, incomplete, outdated, or biased datasets can produce inaccurate security decisions.

False positives: Legitimate activities may be incorrectly classified as malicious, creating unnecessary alerts or service interruptions.

False negatives: Sophisticated attackers may evade AI models, especially when attacks differ significantly from training data.

Adversarial attacks: Attackers can target the AI system through poisoning, evasion, manipulation, or model exploitation.

Model drift: Changes in enterprise behavior and cloud workloads can gradually reduce model accuracy.

Explainability limitations: Complex deep-learning systems may make decisions that are difficult for analysts to interpret.

Privacy concerns: Security monitoring can involve sensitive information about users, customers, applications, and organizational activities.

Computational requirements: Real-time AI analysis of large cloud environments can require significant processing and storage capacity.

Integration complexity: AI systems must interact with IAM, SIEM, SOAR, endpoint security, cloud platforms, application systems, and network controls.

Automation risk: Incorrect automated responses can disrupt legitimate mission-critical services.

Specialized skills: Organizations require professionals who understand cybersecurity, cloud architecture, data engineering, and AI.

Governance burden: AI models require continuous validation, monitoring, documentation, auditing, and risk management.

Changing threat landscape: Attackers continually modify their techniques, meaning that no AI model can remain effective without continuous evaluation and adaptation.

IV. RESULTS AND DISCUSSION

The results demonstrate that integrating artificial intelligence (AI)-driven threat detection with a resilient cloud security architecture can significantly strengthen the protection of modern enterprise systems. Contemporary organizations increasingly depend on public, private, and hybrid cloud environments to support applications, data processing, remote work, digital services, and business-critical operations. This distributed architecture provides scalability and flexibility but also expands the attack surface through cloud APIs, identities, containers, virtual machines, storage services, endpoints, and interconnected applications. Conventional security mechanisms that depend primarily on predefined signatures and perimeter-based controls are less effective against sophisticated attacks that exploit legitimate credentials, unknown vulnerabilities, misconfigured services, and abnormal application behavior. The findings indicate that AI-based detection can address these limitations by continuously analyzing large volumes of security telemetry and identifying deviations from established behavioral patterns. Machine learning models can correlate authentication events, network activity, application logs, endpoint behavior, cloud configuration changes, and data-access patterns to identify potentially malicious activity. This capability allows security teams to detect complex attack sequences rather than responding only to individual alerts. For example, an isolated failed login may have little significance, but repeated authentication failures followed by successful access from an unusual device, privilege escalation, and abnormal database queries can represent a strong indicator of account compromise. AI-based correlation can identify this sequence and assign a higher risk score to the combined activity. The results therefore suggest that intelligent detection provides greater contextual awareness than isolated rule-based monitoring. However, successful implementation depends on the availability and quality of security data. Organizations with fragmented logging, incomplete asset inventories, inconsistent identity information, or poorly integrated security tools may limit the effectiveness of AI models. Consequently, AI-driven threat detection should be implemented on top of a strong cloud security foundation that provides comprehensive visibility and trustworthy telemetry across the enterprise environment.

A second major result concerns the ability of AI to improve security operations through faster alert analysis, prioritization, and response. Modern enterprise systems can generate extremely large numbers of security events, making it difficult for security analysts to identify the most important incidents manually. High alert volumes can create fatigue and increase the possibility that serious threats will be overlooked. AI can reduce this problem by classifying events according to behavioral risk, asset importance, attack context, and historical patterns. Intelligent

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

security platforms can distinguish between routine operational activity and events that demonstrate characteristics associated with compromise. They can also correlate events across multiple cloud accounts, applications, endpoints, and network segments to construct a broader incident narrative. The results indicate that such capabilities can reduce investigation time and improve the efficiency of security operations centers. AI-driven security orchestration can further accelerate response by automatically initiating predefined actions when confidence in a threat assessment is sufficiently high. These actions may include isolating a compromised endpoint, restricting suspicious network communication, disabling a compromised account, forcing credential rotation, or increasing authentication requirements. For enterprise environments, faster containment can significantly reduce the potential impact of an attack. Nevertheless, the findings also highlight the risks of excessive automation. A false positive affecting a critical production workload could create an outage that is itself harmful to the organization. Therefore, resilient security architecture should incorporate risk-based automation, where low-impact and high-confidence responses can occur automatically while high-impact decisions require human authorization. AI should provide analysts with prioritized evidence, recommended actions, and contextual explanations rather than functioning as an uncontrolled autonomous decision-maker. Auditability is also essential, allowing organizations to record how threats were identified, what evidence influenced the decision, and which automated or human actions were performed. This combination of automation and oversight creates a more reliable operational model in which AI provides speed and scale while human experts maintain strategic control.

The results further demonstrate that resilient cloud security requires an identity-centric and zero-trust approach integrated with AI-driven behavioral analysis. In modern cloud environments, users, administrators, applications, service accounts, APIs, and automated workloads may access resources from multiple locations and devices. Consequently, network location alone cannot reliably determine whether a request is trustworthy. AI can strengthen identity security by continuously analyzing authentication patterns, device characteristics, geographic context, privilege usage, resource sensitivity, session behavior, and historical activity. This enables adaptive access decisions in which security requirements respond dynamically to changing risk. A legitimate user accessing ordinary resources from a recognized device may present minimal risk, while the same identity requesting administrative access to sensitive infrastructure from an unfamiliar environment may require additional verification. AI can also identify dormant accounts, excessive permissions, unusual service-account activity, and unexpected privilege escalation. These capabilities can limit the consequences of compromised credentials and reduce opportunities for lateral movement. Resilience also requires protection at the application and infrastructure levels. AI-based security tools can identify vulnerable dependencies, insecure APIs, misconfigured cloud storage, exposed services, suspicious container behavior, and abnormal workload activity. Importantly, risk prioritization should consider business context rather than vulnerability severity alone. A vulnerability in an isolated development system may represent less immediate risk than a moderately rated vulnerability in a publicly accessible application connected to sensitive enterprise databases. AI can combine vulnerability information with asset criticality, exposure, connectivity, and observed attack behavior to improve remediation prioritization. The findings therefore support an integrated architecture in which identity security, application security, infrastructure monitoring, vulnerability management, and behavioral analytics operate together. This approach reduces security silos and provides organizations with a more complete understanding of risk across distributed cloud environments.

Finally, the findings indicate that resilience depends on the ability of the security architecture to continue operating during attacks and recover effectively after security incidents. Threat detection alone is insufficient if an organization cannot contain damage, preserve essential services, and restore affected systems. A resilient cloud security architecture should therefore incorporate network segmentation, redundancy, encryption, secure configuration management, immutable backups, disaster recovery, continuous vulnerability assessment, and tested incident-response procedures. AI can enhance these capabilities by identifying abnormal infrastructure conditions, predicting potential service risks, prioritizing recovery resources, and supporting attack simulations. However, the use of AI introduces additional security concerns. Models can be targeted through adversarial examples, data poisoning, model manipulation, unauthorized access, or malicious inputs designed to evade detection. Organizations must therefore protect AI models, training datasets, inference systems, and security decision interfaces as critical assets. Governance mechanisms should define how models are trained, validated, monitored, updated, and audited. The results also indicate that AI-driven security should be evaluated using operational metrics such as detection accuracy, false-positive rates, mean time to detect, mean time to respond, containment duration, service availability, recovery time, and analyst workload. These measurements provide a more realistic assessment of whether AI improves organizational resilience. Overall, the findings support a layered architecture combining AI-driven detection, zero-trust access, identity intelligence, cloud-native controls, automated orchestration, threat intelligence, application security, and recovery capabilities. Such an

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

architecture transforms cybersecurity from a collection of disconnected defensive tools into a continuous resilience process. The most effective model is therefore not one that attempts to eliminate human involvement but one that intelligently combines automated analysis with expert judgment, enabling enterprises to detect threats earlier, respond faster, maintain critical services, and continuously improve their security posture.

V. CONCLUSION

AI-driven threat detection combined with resilient cloud security architecture provides a powerful foundation for protecting modern enterprise systems against increasingly complex and rapidly evolving cyber threats. The analysis demonstrates that the growth of distributed cloud infrastructure has fundamentally changed the cybersecurity environment. Enterprise applications and data are no longer confined to a single data center or controlled network perimeter; instead, they are distributed across cloud providers, remote endpoints, APIs, containers, virtual machines, edge systems, and interconnected services. This environment creates significant opportunities for attackers to exploit identity weaknesses, misconfigurations, vulnerable applications, excessive privileges, and trusted communication channels. Traditional security approaches based mainly on static rules and known signatures cannot provide sufficient protection against all of these risks. AI-driven threat detection addresses this challenge by continuously analyzing security telemetry and identifying behavioral patterns that may indicate malicious activity. Machine learning can correlate information across multiple security domains, identify anomalies, prioritize suspicious events, and support rapid response. This allows organizations to move toward proactive security in which potential threats are recognized before they develop into major incidents. However, the conclusion is not that AI can independently solve enterprise cybersecurity. Instead, AI should be understood as an intelligent component within a broader security architecture. Strong identity management, encryption, vulnerability management, network segmentation, secure application development, backup protection, and disaster recovery remain essential. AI becomes most valuable when these controls are integrated and provide the data and context required for intelligent analysis. Thus, successful cybersecurity modernization depends on combining advanced analytical capabilities with strong foundational security practices.

A key conclusion is that AI-driven detection can improve the efficiency and effectiveness of enterprise security operations. Modern organizations face an overwhelming volume of security alerts, and manual investigation cannot scale effectively across complex cloud environments. Intelligent analytics can reduce this burden by correlating events, identifying patterns, prioritizing incidents, and providing analysts with meaningful context. Instead of requiring security teams to investigate thousands of unrelated alerts, AI can identify combinations of events that represent credible attack scenarios. This can reduce alert fatigue and enable analysts to focus their attention on high-risk incidents. Automated response can further reduce the time between detection and containment. When a high-confidence threat is identified, predefined actions can immediately restrict access, isolate affected systems, or prevent suspicious communication. Faster response can be particularly important when attackers attempt to move laterally or compromise additional resources. Nevertheless, the analysis emphasizes that automation must be carefully controlled. Security systems operate within business environments where an incorrect decision can disrupt critical services. The most appropriate approach is therefore risk-based automation supported by human oversight. High-confidence, low-impact responses may be automated, while decisions involving critical production systems should receive appropriate human review. Explainability is also important because security analysts need to understand why an AI model considers an activity suspicious. Transparent evidence and confidence scores can help analysts validate AI recommendations and reduce the risk of blindly following automated decisions. The conclusion is therefore that the greatest value of AI lies in human-AI collaboration. Machines provide speed, scale, and continuous monitoring, while human professionals provide contextual understanding, strategic judgment, and accountability.

The study also concludes that resilience requires cybersecurity to extend beyond detection and prevention toward continuous protection, containment, recovery, and learning. A sophisticated enterprise security architecture must assume that some attacks may bypass preventive controls. The organization must therefore be prepared to limit the consequences of compromise and restore operations quickly. Zero-trust security provides an important foundation by requiring continuous evaluation of users, devices, workloads, and access requests rather than automatically trusting entities based on network location. AI can strengthen zero-trust architecture by providing dynamic risk assessments based on behavior and context. Identity analytics can identify unusual authentication, privilege escalation, abnormal service-account behavior, and suspicious resource access. Similarly, AI can improve infrastructure resilience by identifying misconfigurations, vulnerable components, anomalous workload behavior, and unexpected network relationships. However, resilience also requires technical mechanisms such as segmentation, redundancy, immutable backups, disaster recovery, and secure configuration management. These controls reduce the likelihood that a single

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

compromised component will result in widespread operational disruption. Another conclusion is that AI systems themselves must be treated as part of the enterprise attack surface. Their training data, models, interfaces, and automated decision mechanisms require protection against manipulation and unauthorized access. Model governance, continuous validation, adversarial testing, and controlled updates should therefore be incorporated into the security architecture. Enterprises should also measure AI performance using operational indicators rather than relying solely on model accuracy. Detection speed, response time, false-positive rates, service availability, recovery performance, analyst workload, and incident impact provide more meaningful evidence of security value. This resilience-oriented approach ensures that AI contributes to overall organizational continuity rather than focusing narrowly on threat identification.

Ultimately, the study concludes that the future of enterprise cybersecurity depends on intelligent, adaptive, and resilient architectures capable of continuously responding to changing threats and infrastructure conditions. AI-driven threat detection provides the analytical capability required to process large-scale security information and identify patterns that traditional controls may miss. Cloud-native security provides the mechanisms needed to protect distributed applications and infrastructure, while zero-trust principles ensure that access decisions are based on identity and contextual risk rather than assumed trust. Automated orchestration can accelerate response, while human oversight provides the judgment necessary for complex and high-impact decisions. Together, these capabilities can transform cybersecurity from a reactive monitoring function into a continuous organizational resilience capability. Nevertheless, successful implementation requires more than technological investment. Organizations must establish strong governance, improve data quality, train cybersecurity professionals, protect AI systems, define acceptable levels of automation, and continuously evaluate security performance. The architecture must also evolve as cloud environments and attack techniques change. A static security design will eventually become inadequate, regardless of how advanced its initial technology may be. The appropriate objective is therefore continuous adaptation supported by feedback from security incidents, operational experience, threat intelligence, and model performance. AI should not replace cybersecurity professionals or fundamental security controls; rather, it should amplify their effectiveness by providing faster analysis, broader visibility, and intelligent decision support. When integrated with resilient infrastructure, identity-centric security, secure application practices, automated response, and recovery capabilities, AI can substantially strengthen the ability of modern enterprises to protect critical systems. The resulting architecture provides a foundation for secure digital transformation while improving the organization's capacity to withstand, contain, and recover from cyber threats.

VI. FUTURE WORK

Future research should focus on developing adaptive AI models capable of maintaining reliable threat detection as enterprise cloud environments continuously change. Modern organizations frequently modify their infrastructure by adding cloud services, deploying new applications, introducing containers, migrating workloads, and supporting remote users and edge devices. Such changes can alter normal behavioral patterns and make static machine-learning models less effective over time. Future studies should therefore investigate continual-learning architectures that can adapt to new environments without requiring complete retraining. However, adaptive learning creates the possibility of adversarial manipulation, where attackers intentionally introduce malicious data or unusual behavior into the learning process. Future research should develop mechanisms capable of distinguishing legitimate changes from attempts to poison security models. Federated learning could also be investigated as a way to improve threat detection across distributed environments while reducing the need to centralize sensitive security information. Privacy-preserving machine-learning techniques may be particularly valuable for enterprises subject to strict data protection and regulatory requirements. Another research priority is the creation of realistic cloud cybersecurity datasets representing current and emerging threats. Existing datasets may not adequately capture cloud-native attacks involving APIs, identities, serverless applications, containers, service accounts, and multi-cloud environments. Researchers should create benchmark datasets containing realistic attack sequences, legitimate operational behavior, and different levels of threat severity. Evaluation should extend beyond accuracy to include false-positive rates, false-negative rates, detection latency, computational cost, explainability, and robustness against adversarial manipulation. Explainable AI should receive particular attention because cybersecurity analysts must understand why an intelligent system considers an event suspicious. Future models should provide evidence, confidence levels, and contextual relationships that enable analysts to validate automated recommendations. Research should also examine how models can identify previously unseen attacks without producing excessive false alarms. These developments would help establish AI-driven threat detection as a dependable capability rather than a system that performs well only under controlled experimental conditions.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

Future work should also explore intelligent autonomous response mechanisms that can contain threats while minimizing the possibility of operational disruption. Detection without timely containment may have limited value when attackers can move rapidly across distributed enterprise systems. Future AI-driven security architectures could automatically perform actions such as isolating compromised workloads, restricting suspicious accounts, modifying network policies, increasing authentication requirements, or initiating credential rotation. However, autonomous response must account for the criticality of affected systems and the consequences of incorrect decisions. Researchers should therefore investigate confidence-based and risk-aware automation models. In such architectures, the AI system could automatically execute reversible and low-impact actions when confidence is high while requiring human approval for irreversible or business-critical actions. Future research should examine methods for quantifying confidence and operational risk so that automation policies can be dynamically adjusted. AI security agents also require investigation because autonomous systems can themselves become attack targets. Attackers may attempt to manipulate agent instructions, exploit excessive permissions, feed deceptive information into decision processes, or compromise connected security tools. Research should develop secure AI-agent architectures that enforce strict authentication, authorization, tool access, isolation, monitoring, and auditability. Multi-agent cybersecurity is another promising area in which specialized agents could independently analyze identity activity, endpoint behavior, network traffic, application security, and cloud configuration while sharing relevant threat intelligence. Future studies should evaluate whether coordinated agents improve detection and response without creating excessive complexity or new attack pathways. Digital-twin environments could also be used to test autonomous security actions before they are deployed in production. By simulating attacks and potential defensive responses, enterprises could evaluate whether automated decisions would protect systems or unintentionally disrupt critical services. Such research would contribute to safer and more reliable cybersecurity automation.

A third direction for future work involves integrating AI-driven security throughout the application and infrastructure lifecycle. Cybersecurity should not begin after an application has been deployed; security risks should be identified during design, development, testing, deployment, and operation. Future research should examine how AI can analyze source code, software dependencies, infrastructure-as-code templates, API specifications, container images, cloud configurations, and runtime activity as part of an integrated security pipeline. Intelligent systems could identify vulnerabilities and prioritize them according to exploitability, business importance, exposure, and connectivity to sensitive systems. This approach would allow organizations to focus remediation efforts on weaknesses that present the greatest actual risk rather than simply addressing vulnerabilities according to generic severity ratings. Future work should also explore AI-assisted cloud security posture management that continuously detects configuration drift and recommends corrective actions. Integration between vulnerability intelligence and runtime behavior could provide additional context. For example, a vulnerability may receive greater priority if the affected application is externally accessible and is already receiving suspicious requests. Researchers should also examine the role of AI in resilience engineering by developing models that predict service disruption, identify critical dependencies, and recommend recovery strategies. Simulation environments and digital twins could help organizations test whether security controls remain effective during realistic attack scenarios. Future research should also evaluate the economic and organizational consequences of AI-based cybersecurity. Measures such as reduced analyst workload, improved incident-response time, lower downtime, and reduced breach impact can demonstrate whether AI provides practical value. Workforce research should identify the skills required to operate AI-enhanced security systems, including knowledge of cloud architecture, machine learning, threat intelligence, security engineering, and AI governance. Training programs should prepare security professionals to validate AI outputs rather than simply accept automated recommendations.

Finally, future research should address emerging threats created by the convergence of artificial intelligence, cloud computing, edge infrastructure, Internet of Things devices, and advanced cryptographic technologies. Attackers are increasingly able to use automation and AI to conduct reconnaissance, generate convincing social-engineering content, adapt malicious behavior, and identify vulnerable infrastructure. Future studies should therefore examine AI-versus-AI security scenarios in which both attackers and defenders use intelligent systems. Research should determine whether defensive AI can reliably recognize machine-generated attacks and adapt faster than adversarial systems. The development of lightweight AI models for edge and IoT environments should also be investigated because many devices have limited processing capacity and may operate for long periods without security updates. Distributed detection could allow local systems to identify suspicious activity while sharing summarized intelligence with centralized cloud security platforms. Another important research area is post-quantum cybersecurity. As quantum computing develops, existing cryptographic mechanisms may face new challenges, requiring organizations to identify vulnerable algorithms and plan migration strategies. AI could assist with cryptographic asset discovery, prioritization, and migration monitoring. Future research should also investigate the security and privacy implications of large-scale

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

behavioral analytics. Enterprise AI systems may process information about users, employees, customers, and business operations, requiring strict controls over data collection, retention, access, and model usage. Privacy-preserving analytics and transparent governance should therefore become integral to future architectures. Longitudinal studies are particularly important because AI security models must remain effective over extended periods as infrastructure and attack strategies evolve. Future research should evaluate real-world deployments using measures of security effectiveness, resilience, availability, cost, privacy, and human workload. Ultimately, the future of AI-driven cloud security lies in architectures that are adaptive, explainable, resilient, privacy-aware, and governed by humans. Continued research across AI, cloud engineering, cybersecurity, software development, and organizational risk management can enable enterprises to build security systems capable of learning continuously while maintaining the reliability and accountability required for modern digital operations.

REFERENCES

1. Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: A comprehensive review. *Journal of Electrical Systems and Information Technology, 11*, 30. https://doi.org/10.1186/s43067-024-00155-z
2. Gollapudi, R. (2022). Risk-controlled near-zero-downtime Oracle database migration using GoldenGate. International Journal of Computational and Experimental Science and Engineering, 8(3), 113–123. https://doi.org/10.22399/ijcesen.5382
3. Soundappan, S. J. (2024). Deep Learning Enabled Community Cloud Architecture for Intelligent Financial Forecasting and Enterprise Performance Analytics. International Research Journal of Innovative Engineering, 8(5), 15343-15353.
4. Chaba, A. (2018). A platform-independent API integration architecture for scalable enterprise commerce solution. International Journal of Research Publication in Engineering, Technology and Management, 1(1), 9–13.
5. Bellundagi, M. (2023). Design of an Intelligent Clinical Decision Support System Using Machine Learning Techniques. International Journal of Research and Applied Innovations, 6(6), 10075-10081.
6. Juvvadi, R. R. (2017). From record-to-report to insight-to-action: Re-engineering the finance operating model for the cloud ERP era. International Research Journal of Innovative Engineering (IRJIE), 1(2), 371–376.
7. Anand, L. (2024). AI-Powered Cloud Cybersecurity Architecture for Risk Prediction and Threat Mitigation in Healthcare and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(Special Issue 1), 5-12.
8. Gummadi, V. P. K. (2021). Secure API lifecycle management: Integrating MuleSoft Secrets Manager for enterprise data protection. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 537-540.
9. Vani, M., & Dadlani, D. (2023). Smart home – "Aashraya" IoT automation system. International Journal of Computer Technology and Electronics Communication, 6(1), 6393–6403.
10. Vollem, S. (2023). Artificial intelligence for root cause analysis in cloud-native systems: Techniques, architectures, and research trends. European Journal of Advances in Engineering and Technology, 10(9), 120-129.
11. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
12. Singh, I. K. (2024). DevSecOps for enterprise ontology platforms: Continuous validation, security, and compliance of semantic knowledge systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(2), 10359-10369.
13. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
14. Challa, R. (2023). Reliability Engineering for Zero-Downtime Integration of HPC Systems into Regulated Environments. International Journal of Research and Applied Innovations, 6(6), 10082-10092.
15. Macha, Y. (2022). A Review of Cloud-Based CRM Systems in Healthcare: Advances, Tools, Challenges, and Best Practices. Int. J. Curr. Eng. Technol, 12(6), 848-856.
16. Anbazhagan, R. S. K. (2016). A Proficient Two Level Security Contrivances for Storing Data in Cloud.
17. Alex Mathew. (2023). Threat defense through cyber fusion. International Journal of Computer Science and Mobile Computing, 12(1), 24–27. https://doi.org/10.47760/ijcsmc.2022.v12i01.003
18. Kanji, R. K. (2021). Federated data governance framework for ensuring quality-assured data sharing and integration in hybrid cloud-based data warehouse ecosystems through advanced ETL/ELT techniques. International Journal of Computer Techniques, 8(3), 1-9.
19. Awopejo, T. E., Adigun, P. O., & Oyekanmi, T. T. (2023). Emerging applications of artificial intelligence and machine learning in modern earthquake science. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8142–8154.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 8, Issue 6, November-December 2024|

DOI:10.15680/IRJIE.2024.0806002

20. Sivakumer, D. (2024). The impact of technology industry layoffs on project managers: An empirical study in the USA. International Journal of Research and Applied Innovations (IJRAI), 7(4), 11166–11177.
21. Seetala, S. R. (2018). A comprehensive framework for cloud migration of enterprise data warehouses: Architectural transformation, performance optimization, and governance considerations. International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), 4(1), 1861-1878.
22. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
23. Shekhar, P. C. (2022). Accelerating agile quality assurance with AI-powered testing strategies. International Journal of Scientific Research in Engineering and Management, 6(1), 1–11.
24. Reddy, B. P. (2021). Optimizing smart grid performance using Machine Learning: A Data-Driven Approach to Energy Efficiency. J. Electrical Systems, 17(4), 149-156.
25. Narapareddy, V. S. R. (2022). Strategies for Integrating Services with External Systems Via Rest & Soap. Universal Library of Engineering Technology, (Issue).
26. Vani, M., & Dadlani, D. (2023). Smart home – "Aashraya" IoT automation system. International Journal of Computer Technology and Electronics Communication, 6(1), 6393–6403.
27. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
28. Awopejo, T. E., Adigun, P. O., & Oyekanmi, T. T. (2023). Emerging applications of artificial intelligence and machine learning in modern earthquake science. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8142–8154.
29. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
30. Wadhwa, R. (2023). Designing scalable enterprise systems using event-driven microservices and distributed data architecture for high-throughput business applications. International Journal of Computer Engineering and Technology, 14(3), 323-337.
31. Karnam, V. S. (2024). Adaptive and federated test automation using AI in distributed multi-cloud and hybrid infrastructure environments. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 111–121.
32. Ramaswamy, Y. (2023). Ethical and sustainable software delivery: toward green DevOps practices in cloud-native environments. Int. J. Commun. Networks and Inf. Secur, 15(12), 50-59.
33. Abd-Rouf, M. S. K., Adigun, P. O., Alalade, E. O., Oyekanmi, T. T., Faniyi, A. J., Oladapo, B., Awopejo, T. E., Adegoke, O. S., Jamiu, A., Michael, O. B., Obisesan, A., Ajala, S., Adekanye, M. A., Yambali, P. M., & Abd-Rouf, A. B. (2024). From molecular profiling to predictive algorithms: A conceptual machine-learning framework for mechanism-informed therapy selection in multidrug-resistant cancer. International Journal of Science, Research and Technology (IJSRAT), 7(3), 12085–12101.
34. Beeram, S. (2023). Energy efficiency and carbon-aware workload scheduling in Azure. International Journal of Future Innovative Science and Technology (IJFIST), 6(5), 11376–11378.
35. Hoque, M. J., Akter, F., & Mohammad, A. R. (2019). Data-Driven Decision Support System for Restaurant Business Optimization. American Journal of Economics and Business Management, 2(2).
36. Kale, P. (2023). A Federated Learning Approach to Distributed DevOps Automation in Platform Engineering Architectures. International Journal of AI, BigData, Computational and Management Studies, 4(4), 200-208.
37. Soundappan, S. J. (2023). Machine Learning Based Predictive Models for Secure Financial Transactions and Cyber Threat Detection. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(1), 5966-5975.
38. Anbazhagan, R. S. K. (2016). A Proficient Two Level Security Contrivances for Storing Data in Cloud.
39. Bandhela, R. R., & Kundavaram, R. R. (2024). Leveraging machine learning algorithms for real-time health risk assessment and personalized treatment in the US healthcare system. South Eastern European Journal of Public Health, 24, 2218-2229.
40. Rajula, A. (2024). Drift-aligned personalization for privacy-preserving edge health monitoring. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(5), 8895–8906.
41. Gujarathi, M. (2024). Monolith-to-microservices migration in enterprise operations platforms: A workflow-oriented architecture. International Journal of Research Publications in Engineering, Technology and Management, 7(1), 10018–10029.