Int. j. adv. multidisc. res. stud. 2023; 3(1):1481-1490

Received: 03-01-2023
Accepted: 13-02-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Proactive Threat Intelligence and Detection Model Using Cloud-Native Security Tools

[1] Theophilus Onyekachukwu Oshoba, [2] Kabir Sholagberu Ahmed, [3] Olushola Damilare Odejobi
[1, 2, 3] Independent Researcher, Lagos, Nigeria

Corresponding Author: **Theophilus Onyekachukwu Oshoba**

Abstract
As enterprises increasingly migrate workloads to cloud platforms, the threat landscape has evolved with greater sophistication and velocity. Traditional reactive security models, reliant on post-incident response, are insufficient to address modern attack vectors such as identity compromise, misconfigured cloud services, and lateral movement within hybrid environments. This study proposes a Proactive Threat Intelligence and Detection Model leveraging cloud-native security tools to provide real-time monitoring, early threat identification, and automated mitigation. The model integrates threat intelligence feeds, machine learning, and anomaly detection to deliver predictive insights, enabling organizations to act before threats materialize into security incidents. The model begins with a data collection phase, centralizing telemetry from cloud workloads, applications, network logs, and identity services. External threat intelligence feeds augment internal data, enriching the context for detection. In the analysis phase, AI-driven correlation and behavioral analytics identify deviations from normal activity, flagging potential indicators of compromise (IoCs) and suspicious patterns. Risk scoring and prioritization mechanisms allow security teams to focus on high-impact threats, reducing alert fatigue and optimizing resource allocation. The response phase incorporates automated remediation, such as account suspension, workload isolation, or conditional access enforcement, while retaining human-in-the-loop oversight for complex scenarios. Continuous monitoring and feedback loops refine detection algorithms over time, adapting to evolving threats and organizational changes. By leveraging cloud-native security platforms—such as Microsoft Defender, AWS GuardDuty, or Google Chronicle—the model provides scalable, integrated, and real-time security coverage across IaaS, PaaS, and SaaS environments. This proactive approach enhances enterprise resilience by shifting from reactive incident response to predictive threat management. The proposed model ensures early detection, minimizes operational disruption, and supports compliance with regulatory standards. Ultimately, it positions organizations to leverage cloud-native capabilities, integrate AI-driven threat intelligence, and maintain robust, adaptive, and proactive cybersecurity frameworks in complex, hybrid, and multi-cloud environments.

Keywords: Anomaly Detection, Intrusion Detection, Cloud-Native Security, Continuous Monitoring, Behavioral Analytics, Machine Learning, Artificial Intelligence, Log Correlation, SIEM Integration, SOAR Automation, Identity Protection, Endpoint Security, Workload Protection, Vulnerability Management

1. Introduction

The modern enterprise cybersecurity landscape is undergoing a dramatic transformation, driven by the rapid adoption of cloud computing, software-as-a-service (SaaS) platforms, and hybrid cloud architectures (Abisoye and Akerele, 2022; Eboseremen *et al*., 2022). While these technologies provide significant operational efficiency, scalability, and flexibility, they also introduce complex security challenges. Cyber threats targeting cloud environments are becoming increasingly sophisticated, leveraging techniques such as identity compromise, lateral movement, API exploitation, and misconfigured cloud services (Eyinade *et al*., 2022; Kufile *et al*., 2022). Attackers exploit vulnerabilities in multi-tenant architectures, weak access controls, and inadequate monitoring to gain unauthorized access, exfiltrate sensitive data, and disrupt critical business operations (Abisoye and Akerele, 2022; Eboseremen *et al*., 2022).

Traditional security models, which rely heavily on reactive incident response and perimeter-based defense mechanisms, are no longer sufficient in this evolving threat landscape (Essien *et al*., 2022 [24]; Eyinade *et al*., 2022). Reactive approaches often

detect threats only after an attack has occurred, limiting an organization's ability to mitigate damage in a timely manner. Moreover, these models struggle to provide visibility into dynamic cloud environments where workloads, users, and resources are constantly changing (Abisoye *et al*., 2022 [3]; Kufile *et al*., 2022). The limitations of legacy security frameworks underscore the need for proactive, intelligent approaches that can anticipate threats and respond in near real-time (Ogedengbe *et al*., 2022; Omolayo *et al*., 2022 [57]).

The motivation for this, lies in addressing these gaps through proactive threat intelligence and detection. By leveraging cloud-native security tools, enterprises can shift from a reactive stance to a predictive security posture. Cloud-native tools such as Microsoft Defender, AWS GuardDuty, and Google Chronicle provide real-time telemetry, integrated threat intelligence, automated alerting, and machine learning-based anomaly detection. These capabilities enable organizations to identify potential threats before they escalate into security incidents, thereby minimizing operational disruption and reducing the risk of data breaches. Proactive threat management also enhances compliance with regulatory frameworks, strengthens organizational resilience, and supports continuous monitoring of dynamic cloud resources (Chima *et al*., 2022; Eyinade *et al*., 2022).

The primary purpose of this, is to develop a Proactive Threat Intelligence and Detection Model specifically tailored for cloud-based environments. The proposed model aims to integrate diverse sources of threat intelligence, leverage machine learning and behavioral analytics, and employ automated response mechanisms to ensure timely mitigation of risks. By combining predictive detection with real-time monitoring, the model seeks to improve visibility, accelerate incident response, and optimize the use of security resources across complex cloud infrastructures (Okiye *et al*., 2022; Nwokediegwu *et al*., 2022 [48]).

The scope of this, encompasses enterprise cloud deployments, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) solutions. It focuses on the integration of cloud-native security tools and services to provide scalable, automated, and adaptive threat intelligence and detection capabilities. The model addresses critical aspects such as centralized telemetry collection, AI-driven anomaly detection, risk prioritization, automated remediation, and continuous feedback loops. Additionally, it considers the operational and compliance requirements of enterprises, ensuring that security measures are both effective and aligned with industry standards.

The shift toward cloud-first and hybrid IT strategies necessitates a proactive, intelligence-driven approach to cybersecurity. The proposed model aims to empower organizations to anticipate, detect, and respond to emerging threats in real-time, leveraging cloud-native tools to enhance operational resilience and maintain robust security across dynamic enterprise environments.

2. Methodology

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology was applied to develop a proactive threat intelligence and detection model using cloud-native security tools. The process began with a systematic identification of relevant literature and resources across multiple academic and industry databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus, supplemented by white papers, vendor documentation, and security-focused reports from cloud providers such as Microsoft, AWS, and Google Cloud. Search terms employed Boolean operators and combinations such as "threat intelligence," "cloud-native security," "proactive detection," "SIEM," "SOAR," "cloud security analytics," and "cyber threat monitoring." The initial search yielded a broad set of publications addressing cloud security frameworks, threat intelligence systems, automated detection techniques, and incident response in cloud environments.

Screening was conducted to remove duplicates and assess relevance. Only peer-reviewed publications, authoritative technical reports, and vendor-provided guidelines published between 2015 and 2025 were retained to ensure currency and practical applicability. Studies focusing solely on on-premises threat detection, legacy SIEM-only systems, or consumer-level security tools were excluded.

Eligibility was determined through full-text review against inclusion criteria. Sources were required to provide empirical, theoretical, or methodological insights into proactive threat detection, automated alerting, threat intelligence integration, or security orchestration in cloud-native environments. Exclusion criteria eliminated studies that lacked practical relevance to cloud-native deployment, did not address detection or intelligence frameworks, or were purely conceptual without implementation considerations.

Included studies were systematically analyzed to extract data related to security tool integration, automated threat detection, anomaly analytics, incident response workflows, and proactive mitigation strategies. The synthesis of these data informed the development of a proactive threat intelligence and detection model that integrates multiple cloud-native security tools, leverages real-time telemetry, and supports automated threat correlation, prioritization, and response.

The PRISMA methodology ensured transparency, reproducibility, and rigor in selecting, evaluating, and synthesizing relevant evidence, minimizing selection bias while maximizing coverage of both theoretical and practical perspectives. The resulting model reflects a systematic, evidence-based approach for proactively identifying, analyzing, and mitigating security threats in cloud environments, providing enterprises with actionable intelligence and automated response capabilities that enhance overall security posture.

2.1 Conceptual Foundations

Threat intelligence refers to the systematic collection, analysis, and dissemination of information regarding potential or active cyber threats that could impact an organization. Its primary objective is to enhance situational awareness, inform decision-making, and enable proactive measures to prevent or mitigate security incidents (Ezeilo *et al*., 2022; Okiye *et al*., 2022). Threat intelligence is derived from both internal and external sources. Internal sources include logs, security information and event management (SIEM) systems, endpoint detection and response (EDR) telemetry, and historical incident reports. External sources encompass threat feeds, industry sharing platforms, governmental advisories, and open-source intelligence

(OSINT). Real-time threat intelligence is particularly valuable, as it enables organizations to respond to emerging threats before they manifest into operational disruptions or data breaches.

Structured threat data is central to effective threat intelligence. This includes Tactics, Techniques, and Procedures (TTPs), which describe the methods and approaches used by attackers; Indicators of Compromise (IoCs), such as malicious IP addresses, hashes, or URLs; and detailed attack patterns, which provide insight into adversary behavior and potential attack chains. By systematically organizing this information, security teams can prioritize threats, correlate events across multiple data sources, and design targeted mitigation strategies (Akindemowo *et al*., 2022 [6]; Kufile *et al*., 2022).

Cloud-native security tools are designed to operate seamlessly within cloud environments, leveraging the inherent scalability, elasticity, and integration capabilities of cloud platforms. These tools provide native monitoring, logging, and alerting, collecting telemetry from workloads, applications, and identity services across IaaS, PaaS, and SaaS deployments. Centralized logging ensures that security events are captured consistently, enabling comprehensive visibility into user activities, network traffic, and system behaviors (Bukhari *et al*., 2020 [11]; Ezeilo *et al*., 2022).

Modern cloud-native platforms incorporate machine learning and anomaly detection to identify patterns that deviate from baseline behavior. For instance, unusual login locations, abnormal access volumes, or unexpected privilege escalations can trigger automated alerts. In addition, these tools often support automated response workflows, such as temporarily blocking accounts, isolating compromised workloads, or enforcing conditional access policies (Didi *et al*., 2022 [21]; Okuboye, 2022). Automation reduces the time between detection and mitigation, allowing organizations to respond at scale without overburdening human operators.

Popular examples of cloud-native security tools include Microsoft Defender for Cloud, AWS GuardDuty, and Google Chronicle, each offering integration with their respective cloud services, native telemetry collection, and AI-driven threat analysis. By leveraging these platforms, enterprises can achieve real-time visibility, reduce detection latency, and improve the accuracy of threat identification (Ogedengbe *et al*., 2022; Nwokocha *et al*., 2022 [49]).

Traditional cybersecurity approaches are largely reactive, focusing on identifying and mitigating threats after an incident occurs. Proactive detection shifts the paradigm toward predictive security, emphasizing early identification of potential threats and timely intervention. Core principles of proactive detection include early warning, continuous monitoring, and automated mitigation.

Early warning involves leveraging threat intelligence and anomaly detection to anticipate attacks before they impact critical systems. By correlating IoCs, TTPs, and behavioral patterns, security teams can identify threats in their initial stages, preventing escalation and minimizing operational impact.

Continuous monitoring ensures that enterprise cloud environments are observed in real-time, capturing deviations from normal behavior and providing immediate insights into emerging threats (Kufile *et al*., 2022; Ubamadu *et al*., 2022 [60]). This approach reduces blind spots and enables dynamic adaptation to changing risk conditions.

Automated mitigation complements early warning and continuous monitoring by enabling rapid, policy-driven responses to detected threats. Automated actions, such as enforcing MFA challenges, isolating workloads, or revoking access, help contain potential compromises before they propagate across the environment. This combination of intelligence, continuous observation, and automated response forms the backbone of a proactive security posture, reducing reliance on manual intervention and improving overall resilience.

The conceptual foundation of a proactive threat intelligence and detection model integrates structured threat intelligence, cloud-native security tools, and predictive detection principles. Threat intelligence provides the knowledge framework for understanding adversary behavior, while cloud-native tools operationalize monitoring, analysis, and automated response at scale (Okuboye, 2022; Akhamere, 2022). Proactive detection principles ensure that organizations move beyond reactive alerting, enabling early warning, continuous observation, and rapid mitigation of emerging threats. Together, these components establish a robust framework for securing enterprise cloud environments against increasingly sophisticated and dynamic cyber threats.

2.2 Threat Landscape in Cloud Environments

As enterprises increasingly migrate critical workloads to cloud infrastructures, understanding the evolving threat landscape in cloud environments has become essential for designing effective security and detection strategies. Cloud computing introduces unique architectural, operational, and management characteristics that expose organizations to a range of specialized attack vectors, insider risks, and shared-responsibility challenges as shown in Fig 1 (Ilufoye *et al*., 2022 [37]; Kufile *et al*., 2022). Proactive threat intelligence and detection models must account for these nuances to maintain robust security postures.

Cloud-specific attack vectors constitute one of the primary categories of risk. Misconfigurations, such as publicly exposed storage buckets, overly permissive identity and access management (IAM) roles, or improperly secured virtual networks, remain among the most prevalent sources of compromise. Attackers frequently exploit these configuration errors to gain unauthorized access to sensitive data or cloud services. Identity compromise is another critical vector, where stolen or phished credentials provide attackers with the means to infiltrate cloud accounts, escalate privileges, and conduct lateral movement within the environment. Unlike traditional on-premises networks, cloud systems often combine multiple regions, tenants, and virtual networks, creating complex topologies that can obscure malicious activity and complicate detection. Lateral movement in cloud environments can be accelerated by the pervasive use of centralized identity systems and shared resources, enabling attackers to pivot rapidly across services and workloads once a foothold is established.

Insider threats and privileged access exploitation further amplify cloud security risks. Employees, contractors, or third-party administrators with elevated privileges can intentionally or inadvertently expose sensitive data or disrupt operations. The extensive delegation of administrative capabilities in cloud platforms, combined with insufficient monitoring or segregation of duties, increases the attack surface for insiders. Malicious insiders may exfiltrate data, modify configurations to weaken

security controls, or bypass audit trails, while unintentional misuse, such as misapplying security policies, can create vulnerabilities that external actors can exploit (Odinaka *et al*., 2022; Ayumu and Ohakawa, 2022) [50, 9]. Detection strategies must, therefore, incorporate behavioral analytics and anomaly detection to identify unusual access patterns or privilege escalation attempts.

API and microservices security risks represent another dimension of cloud-specific threats. Modern cloud applications often rely on API-driven architectures and microservices for scalability, integration, and automation. While these paradigms enhance operational efficiency, they also introduce new vulnerabilities. Insecure API endpoints, improper authentication or authorization, and inadequate rate-limiting mechanisms can expose critical services to exploitation. Attackers targeting APIs may perform privilege escalation, data exfiltration, or service disruption, while microservices' distributed nature complicates monitoring and forensic investigation. Ensuring secure API design, enforcing authentication standards, and continuously monitoring API traffic are essential components of proactive threat management.

The multi-tenant architecture and shared responsibility model inherent in cloud environments further shape the threat landscape. Multi-tenancy enables cost-effective resource sharing but introduces risks associated with resource isolation, noisy neighbors, and potential cross-tenant attacks. Exploitation of vulnerabilities in underlying hypervisors or container orchestrators could allow attackers to compromise multiple tenants or access shared infrastructure (Akhamere, 2022; Filani *et al*., 2022). The shared responsibility model, which delineates security obligations between cloud providers and customers, requires enterprises to maintain vigilant oversight of their configurations, data, and application security, while relying on providers for infrastructure-level protections. Misunderstandings of these responsibilities can lead to gaps in detection and mitigation, emphasizing the need for clearly defined policies, continuous monitoring, and alignment with provider security guidance.

The threat landscape in cloud environments is characterized by a combination of cloud-specific attack vectors, insider threats, API and microservices vulnerabilities, and the complexities of multi-tenant and shared responsibility architectures. Misconfigurations, identity compromise, and lateral movement can facilitate rapid exploitation of cloud resources, while privileged insider access and API vulnerabilities present persistent risks that are challenging to detect. Multi-tenancy and shared responsibility further complicate threat management, requiring coordinated governance between enterprises and providers (Dako *et al*., 2019; Mgbame *et al*., 2022). Understanding these factors is essential for developing proactive threat intelligence and detection models capable of identifying, analyzing, and mitigating emerging cloud threats, thereby safeguarding enterprise workloads and sensitive data in dynamic, distributed cloud infrastructures.

2.3 Proactive Threat Intelligence and Detection Model Framework

The rapidly evolving cyber threat landscape in cloud environments necessitates a structured and methodical approach to threat intelligence and detection. The proposed Proactive Threat Intelligence and Detection Model Framework is designed to provide enterprises with real-time visibility, predictive insights, and rapid mitigation capabilities (Dako *et al*., 2019; Davidor *et al*., 2022). The framework is divided into four critical phases: data collection, analysis, response, and continuous monitoring with feedback as shown in Fig 2. Each phase is integral to ensuring a holistic, adaptive, and resilient security posture for modern cloud deployments.

The foundation of the framework lies in comprehensive and centralized data collection. Enterprises must aggregate telemetry from a diverse array of cloud resources, including virtual machines, containers, applications, APIs, and identity services. Centralized logging ensures consistent visibility across infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) environments, enabling detection of anomalies, unauthorized access attempts, and policy violations.

Integration of external threat feeds and industry intelligence enhances situational awareness. These feeds provide real-time information on emerging threats, indicators of compromise (IoCs), and adversary tactics, techniques, and procedures (TTPs). Combining internal telemetry with external intelligence enables enriched threat context, allowing security teams to prioritize high-risk events and anticipate attack patterns. By structuring data efficiently and maintaining robust logging pipelines, the framework ensures that raw telemetry is transformed into actionable intelligence, serving as the basis for predictive threat detection and informed decision-making.

Once data is collected, the analysis phase applies advanced computational techniques to transform raw events into actionable insights. Machine learning and AI-driven correlation are employed to detect subtle patterns, relationships, and anomalies across users, applications, and network activity. These technologies can identify deviations from baseline behaviors that may indicate compromised accounts, insider threats, or lateral movement attempts.

Behavioral analytics play a central role in understanding normal activity patterns and detecting deviations. By analyzing historical and real-time user activity, access patterns, and system interactions, behavioral models can flag anomalous events such as unusual login locations, abnormal data transfers, or unexpected privilege escalations. The combination of machine learning and behavioral analytics enhances detection accuracy, reduces false positives, and provides actionable insights for timely intervention (Bukhari *et al*., 2022; Onalaja *et al*., 2022) [12, 58].

Prioritization of threats is also essential. Using risk scoring and potential impact assessment, the framework evaluates which events warrant immediate attention. High-risk activities—such as attempts to access sensitive data or compromise privileged accounts—are escalated for immediate response, while lower-risk anomalies can be monitored continuously. This prioritization ensures optimal allocation of security resources and supports strategic decision-making under dynamic conditions.

The response phase operationalizes the insights generated during analysis. Automated remediation mechanisms, guided by predefined playbooks, allow immediate action to contain or neutralize threats. Examples include account lockdowns, isolation of compromised workloads, revocation of access rights, and deployment of conditional access policies. Automation reduces the time between detection and mitigation, minimizing potential damage and

operational disruption.

Human-in-the-loop escalation complements automated actions for complex or high-risk scenarios. Security teams intervene when contextual judgment is required, such as evaluating potential business impact, coordinating cross-departmental response, or analyzing sophisticated attack vectors. Combining automation with expert oversight ensures both rapid response and intelligent decision-making.

Additionally, the framework emphasizes threat intelligence sharing and feedback loops. Post-incident analysis informs the refinement of detection rules, adjustment of risk scoring models, and incorporation of new TTPs into intelligence feeds. By continuously learning from both internal and external events, the framework evolves in response to the changing threat landscape, increasing resilience over time (Chima *et al*., 2022; Ayodeji *et al*., 2022 [8]).

Continuous monitoring is a cornerstone of proactive threat management. Real-time dashboards, alerts, and audit trails provide security teams with comprehensive visibility into cloud activities and potential security incidents. These monitoring mechanisms enable rapid identification of anomalous behavior and maintain compliance with regulatory standards.

Periodic evaluation of detection rules and intelligence sources ensures that the framework remains effective. Threats evolve rapidly, and static detection rules may become obsolete. By regularly assessing the performance of detection algorithms, updating anomaly thresholds, and integrating emerging threat intelligence, the system maintains its predictive accuracy.

Adaptive learning further strengthens the framework. Machine learning models and behavioral analytics are continuously refined based on feedback from both automated responses and human analysis. This iterative process enables the framework to improve its detection capabilities over time, identifying novel attack patterns and minimizing false positives. Continuous adaptation ensures that the threat intelligence and detection system remains aligned with evolving enterprise requirements and cloud architectures.

The Proactive Threat Intelligence and Detection Model Framework provides a structured, adaptive, and scalable approach to securing cloud environments. By integrating centralized data collection, AI-driven analysis, automated and human-guided response, and continuous monitoring with feedback, the framework enables enterprises to transition from reactive to predictive security postures. Leveraging cloud-native security tools and real-time threat intelligence, organizations can detect anomalies early, prioritize high-risk events, automate remediation, and continuously refine detection capabilities. This comprehensive approach enhances operational resilience, mitigates risks, and ensures that enterprise cloud infrastructures remain secure, compliant, and capable of responding to increasingly sophisticated cyber threats (Davidor *et al*., 2022; Filani *et al*., 2022).

2.4 Implementation Considerations

Implementing a proactive threat intelligence and detection model in enterprise cloud environments requires careful attention to technical, operational, and regulatory considerations. The model's effectiveness depends not only on its conceptual framework but also on how it integrates with existing cloud-native tools, scales across large deployments, ensures compliance, and supports multi-cloud interoperability (Kufile *et al*., 2022; Eyinade *et al*., 2022). Each of these aspects is critical to achieving a secure, resilient, and efficient cybersecurity posture as shown in Fig 3.

A key consideration in implementation is seamless integration with cloud-native security tools, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Identity and Access Management (IAM) platforms. SIEM solutions aggregate telemetry from diverse cloud workloads, applications, and identity services, providing centralized logging, correlation, and analytics capabilities. Integrating threat intelligence feeds into SIEM enables real-time contextualization of security events and facilitates prioritization of potential incidents based on severity and risk.

SOAR platforms complement SIEM by automating incident response workflows and orchestrating remediation actions. Integration allows the proactive model to implement pre-defined playbooks, such as account lockdowns, workload isolation, or conditional access enforcement, reducing time-to-response and minimizing operational disruption. Similarly, IAM platforms provide the foundation for identity-aware threat detection, allowing monitoring of access patterns, anomalous privilege escalation, and policy violations. Coordinated integration of SIEM, SOAR, and IAM ensures that threat intelligence is actionable, response workflows are automated, and identity-driven attacks are detected and mitigated efficiently.

Enterprise cloud environments are dynamic and can consist of thousands of users, workloads, applications, and geographically distributed resources. Therefore, the implementation of a proactive threat intelligence model must consider scalability and performance. Centralized logging, data collection, and analytics pipelines should be capable of handling high-volume, high-velocity telemetry without introducing latency or processing bottlenecks. Cloud-native platforms inherently provide elastic scaling to accommodate spikes in activity, but careful architectural design is necessary to ensure continuous performance and reliability.

Performance optimization also involves prioritization of high-risk events, filtering redundant or low-priority alerts, and leveraging AI-driven analytics to reduce computational overhead. Distributed processing and parallelized analysis can further enhance throughput, enabling real-time detection and response even in large-scale environments (Mgbame *et al*., 2022; Chima *et al*., 2022). Ensuring scalable and efficient operation is critical to maintaining situational awareness and preventing security gaps in complex enterprise clouds.

Regulatory compliance and data privacy are integral to the deployment of any security model. Organizations must ensure that threat intelligence collection, storage, analysis, and sharing adhere to relevant standards, including ISO 27001, GDPR, HIPAA, and industry-specific mandates. Compliance considerations include secure handling of personally identifiable information (PII), proper data retention policies, and auditability of security actions.

Implementation must also incorporate governance mechanisms for data segregation, encryption, and access controls. For example, security logs and telemetry containing sensitive user data should be anonymized or

pseudonymized where possible, and access to these datasets should be strictly controlled. Ensuring regulatory adherence not only mitigates legal and financial risks but also reinforces stakeholder confidence in the organization's cloud security practices.

Many enterprises operate in multi-cloud environments, utilizing services from multiple providers such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform. Effective implementation requires cross-cloud interoperability, ensuring that the proactive threat intelligence model can collect, correlate, and analyze telemetry across heterogeneous platforms.

Interoperability considerations include standardized log formats, consistent identity and access management policies, and unified threat intelligence integration. API-based data ingestion, cloud-native connectors, and centralized dashboards facilitate comprehensive visibility across clouds. Cross-cloud integration also supports coordinated automated response and threat mitigation, enabling enterprises to maintain a cohesive security posture despite distributed and diverse infrastructure.

Implementing a proactive threat intelligence and detection model requires careful planning and execution across multiple dimensions. Integration with SIEM, SOAR, and IAM platforms ensures actionable intelligence and efficient response workflows. Scalability and performance considerations guarantee real-time detection and analysis in large enterprise environments. Compliance with regulatory standards safeguards data privacy and audit readiness, while cross-cloud interoperability enables unified monitoring and mitigation in multi-cloud deployments. By addressing these implementation considerations, organizations can maximize the effectiveness of cloud-native threat intelligence and detection models, enhancing security, resilience, and operational continuity in complex cloud ecosystems (Filani *et al*., 2022; John and Oyeyemi, 2022 [38]).

2.5 Best Practices

Effective threat intelligence and detection in cloud environments requires a structured, risk-aware approach that integrates technological, organizational, and procedural best practices. Cloud infrastructures, characterized by multi-tenancy, dynamic scaling, and distributed resources, introduce unique security challenges that demand proactive strategies rather than reactive responses. By adopting risk-based prioritization, aligning with zero-trust principles, leveraging automation with oversight, and continuously enriching threat intelligence, enterprises can establish resilient cloud security postures.

A foundational best practice is the risk-based prioritization of assets and threats. Cloud environments often host a diverse array of workloads, ranging from critical enterprise applications and sensitive data stores to less critical development or test environments (Oyeyemi, 2022 [59]; Ayanbode *et al*., 2022). Prioritizing security monitoring and mitigation efforts according to the sensitivity and business impact of assets allows security teams to focus on the highest-risk areas. Threat modeling, vulnerability assessments, and historical incident analysis help identify the most probable and consequential attack vectors. Risk scoring frameworks can guide resource allocation, ensuring that proactive detection mechanisms, such as alerting thresholds, logging granularity, and incident response workflows, are concentrated on critical assets while maintaining visibility across the broader environment.

Alignment with zero-trust principles and identity-centric security is another essential practice. Zero-trust architectures operate under the assumption that no entity—internal or external—should be trusted implicitly. In cloud-native environments, this entails enforcing continuous verification of users, devices, and workloads before granting access to resources. Identity-centric security integrates threat detection with authentication, authorization, and policy enforcement, ensuring that anomalous behaviors, suspicious privilege escalations, or unusual access patterns are rapidly identified and mitigated. Conditional access policies, role-based access control, and continuous risk evaluation support this alignment, reducing the attack surface and limiting the potential for lateral movement across cloud services.

Leveraging automation while maintaining human oversight is critical for scaling proactive detection in complex cloud environments. Automated security tools, including cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms, enable real-time monitoring, alerting, and incident response, minimizing detection latency. Machine learning and behavioral analytics can identify anomalies in user activity, network traffic, or API usage. However, automation must be complemented with human expertise to validate alerts, interpret contextual subtleties, and make strategic decisions during complex incidents. Maintaining this balance ensures efficiency without compromising analytical rigor or introducing excessive false positives that could desensitize security teams.

Continuous threat intelligence enrichment and model tuning further enhance the effectiveness of proactive detection. Cloud environments evolve rapidly, with frequent deployment of new services, applications, and integrations. Regularly updating threat intelligence feeds, incorporating emerging attack patterns, and analyzing internal telemetry data ensures that detection models remain accurate and relevant. Model tuning involves adjusting thresholds, refining risk scoring algorithms, and optimizing correlation rules to minimize false positives and false negatives. Feedback loops, derived from post-incident analyses or penetration testing, provide empirical insights that improve predictive capabilities, enabling security teams to anticipate and mitigate threats before they manifest in operational impact.

Best practices for proactive threat intelligence and detection in cloud environments emphasize a risk-informed, identity-centric, and continuously adaptive approach. Prioritizing high-value assets and probable threats ensures efficient allocation of monitoring and mitigation resources. Zero-trust alignment and identity-based security reduce implicit trust and constrain attack pathways. Automation, complemented by human oversight, enhances scalability and responsiveness, while continuous enrichment and tuning of threat intelligence models maintain detection accuracy in dynamic environments (Bankole Lateefat, 2019 [10]; Dako *et al*., 2019). By integrating these practices, enterprises can strengthen their cloud security posture, proactively identify emerging threats, and respond effectively to both internal and external risks, thereby safeguarding critical workloads and maintaining operational resilience in complex, distributed cloud infrastructures.

2.6 Future Directions

The evolving cybersecurity landscape necessitates continuous innovation in threat intelligence and detection, particularly within cloud environments where attack surfaces are expansive and dynamic. While current cloud-native security tools provide significant capabilities for real-time monitoring and automated response, future developments will increasingly focus on predictive, collaborative, and integrated approaches. Emerging directions for proactive threat intelligence and detection include advanced AI/ML integration, cross-industry threat intelligence sharing, seamless integration with DevSecOps workflows, and proactive simulation of attack scenarios for resilience testing.

The application of advanced artificial intelligence (AI) and machine learning (ML) represents a critical future direction. While existing systems leverage ML for anomaly detection and behavioral analytics, predictive threat modeling can extend these capabilities by anticipating attack vectors before they materialize (Essien *et al*., 2019; Etim *et al*., 2019 [27]). Techniques such as deep learning, reinforcement learning, and graph-based modeling can analyze complex interdependencies across users, workloads, and network activities, identifying subtle patterns indicative of emerging threats. Predictive models can prioritize threats based on potential impact, simulate adversary behavior, and recommend preemptive mitigations, enabling organizations to move from reactive defense to a truly predictive cybersecurity posture.

Collaboration among organizations, industry consortia, and government agencies is another crucial direction for enhancing proactive threat detection. By sharing threat intelligence, including indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs), and attack patterns, enterprises can gain insights into emerging threats that may not yet be visible within their own environments. Cross-industry sharing accelerates response times, improves detection accuracy, and supports collective defense strategies against coordinated attacks. Future models will increasingly integrate standardized intelligence feeds and automated ingestion pipelines, enabling near real-time updates to detection frameworks across organizational boundaries.

Integrating threat intelligence directly into DevSecOps pipelines represents a proactive strategy for mitigating vulnerabilities before deployment. Continuous security monitoring, automated code scanning, and vulnerability assessment integrated into development workflows allow organizations to identify and remediate potential security weaknesses early in the software lifecycle. Cloud-native platforms can leverage API-driven integrations to feed telemetry, risk indicators, and threat intelligence into CI/CD pipelines, ensuring that applications are hardened prior to production. This approach bridges the gap between security and development, enabling real-time enforcement of security best practices while accelerating delivery cycles.

Another future direction involves the proactive simulation of attack scenarios, sometimes referred to as “red teaming” or automated adversary emulation. By simulating realistic attack techniques, organizations can test the effectiveness of detection algorithms, incident response playbooks, and automated mitigation strategies in controlled environments. Coupled with automated resilience testing, this approach enables continuous validation of security controls, identification of gaps, and refinement of detection models. Cloud-native orchestration and containerized environments facilitate large-scale simulations without impacting production workloads, ensuring that enterprises maintain readiness against evolving threats.

The future of proactive threat intelligence and detection is characterized by predictive, collaborative, and integrated approaches. Advanced AI/ML techniques enable anticipatory threat modeling, while cross-industry intelligence sharing strengthens collective defense. Integration with DevSecOps pipelines ensures that security is embedded into the development lifecycle, facilitating early vulnerability detection and remediation. Proactive simulation of attack scenarios and automated resilience testing provide continuous validation of detection and mitigation capabilities, enhancing enterprise readiness and operational resilience. Collectively, these future directions transform cloud-native security from reactive monitoring to a predictive and adaptive framework, positioning organizations to respond dynamically to sophisticated cyber threats while maintaining business continuity, regulatory compliance, and trust in complex cloud ecosystems (Nwokediegwu *et al*., 2019 [47]; Essien *et al*., 2019).

3. Conclusion

Proactive threat intelligence and detection in cloud environments constitute a critical component of modern cybersecurity strategies. The proposed model emphasizes continuous monitoring, integration of cloud-native security tools, and the use of automated intelligence to identify and mitigate threats before they escalate into operational or financial impacts. By combining real-time telemetry, anomaly detection, and risk-based prioritization, the model provides enterprises with actionable insights that enhance situational awareness and enable rapid response to emerging threats.

The strategic benefits of this approach are multifaceted. Early detection of suspicious activities reduces the window of exposure to attacks, limiting potential damage from data breaches, account compromise, or service disruption. By continuously assessing risk across cloud assets and workloads, organizations can proactively allocate resources, apply mitigation controls, and adjust policies to address the most pressing threats. Additionally, the integration of automated detection and response mechanisms enhances operational resilience, allowing security teams to manage complex, distributed environments efficiently without overwhelming human operators. The combination of automation and human oversight ensures accuracy, reduces false positives, and maintains the agility needed to respond to evolving attack vectors.

Looking forward, the vision for cloud-native cybersecurity encompasses adaptive, AI-driven frameworks that integrate threat intelligence, detection, and response across hybrid and multi-cloud environments. Machine learning and predictive analytics will enable anticipatory security measures, while continuous model tuning and enrichment will ensure relevance against emerging threats. The adoption of identity-centric, zero-trust principles, combined with cloud-native automation, will further reduce risk exposure and fortify organizational resilience. In this context, proactive threat intelligence and detection not only address present-day security challenges but also provide a scalable and forward-looking foundation for managing complex,

dynamic cloud infrastructures, ensuring that enterprises remain secure, compliant, and operationally robust in an increasingly digital and distributed landscape.

4. References

1. Abisoye A, Akerele JI. A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res Growth Eval. 2022; 3(1):700-713.
2. Abisoye A, Akerele JI. A scalable and impactful model for harnessing artificial intelligence and cybersecurity to revolutionize workforce development and empower marginalized youth. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(1):714-719.
3. Abisoye A, Udeh CA, Okonkwo CA. The Impact of AI-Powered Learning Tools on STEM Education Outcomes: A Policy Perspective. Int. J. Multidiscip. Res. Growth Eval. 2022; 3(1):121-127.
4. Akhamere GD. Behavioral indicators in credit analysis: Predicting borrower default using non-financial behavioral data. International Journal of Management and Organizational Research. 2022; 1(1):258-266. Doi: https://doi.org/10.54660/IJMOR.2022.1.1.258-266
5. Akhamere GD. Beyond traditional scores: Using deep learning to predict credit risk from unstructured financial and behavioral data. International Journal of Management and Organizational Research. 2022; 1(1):249-257. Doi: https://doi.org/10.54660/IJMOR.2022.1.1.249-257
6. Akindemowo AO, Erigha ED, Obuse E, Ajayi JO, Soneye OM, Adebayo A. A conceptual model for agile portfolio management in multi-cloud deployment projects. International Journal of Computer Science and Mathematical Theory. 2022; 8(2):64-93. IIARD - International Institute of Academic Research and Development. https://iiardjournals.org/get/IJCSMT/VOL.%208%20NO.%202%202022/A%20Conceptual%20Model%20for%20Agile%2064-93.pdf
7. Ayanbode N, Cadet E, Etim ED, Essien IA, Ajayi JO. Deep learning approaches for malware detection in large-scale networks. IRE Journals. 2019; 3(1):483-489. https://irejournals.com/formatedpaper/1710371.pdf
8. Ayodeji DC, Oladimeji O, Ajayi JO, Akindemowo AO, Eboseremen BO, Obuse E, *et al*. Operationalizing analytics to improve strategic planning: A business intelligence case study in digital finance. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):567-578. Doi: https://doi.org/10.54660/.JFMR.2022.3.1.567-578
9. Ayumu MT, Ohakawa TC. Real Estate Portfolio Valuation Techniques to Unlock Funding for Affordable Housing in Africa, 2022.
10. Bankole FA, Lateefat T. Strategic cost forecasting framework for SaaS companies to improve budget accuracy and operational efficiency. IRE Journals. 2019; 2(10):421-432.
11. Bukhari TT, Oladimeji O, Etim ED, Ajayi JO. Advancing data culture in West Africa: A community-oriented framework for mentorship and job creation. International Journal of Multidisciplinary Futuristic Development. 2020; 1(2):1-18.
12. Bukhari TT, Oladimeji O, Etim ED, Ajayi JO. Embedding governance into digital transformation: A roadmap for modern enterprises. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(5):685-707. Doi: https://doi.org/10.32628/IJSRCSEIT
13. Chima OK, Idemudia SO, Ezeilo OJ, Ojonugwa BM, Adesuyi AOMO. Advanced Review of SME Regulatory Compliance Models Across US State-Level Jurisdictions, 2022.
14. Chima OK, Ojonugwa BM, Ezeilo OJ. Integrating Ethical AI into Smart Retail Ecosystems for Predictive Personalization. International Journal of Scientific Research in Engineering and Technology. 2022; 9(9):68-85.
15. Chima OK, Ojonugwa BM, Ezeilo OJ, Adesuyi MO, Ochefu A. Deep learning architectures for intelligent customer insights: Frameworks for retail personalization. Shodhshauryam, International Scientific Refereed Research Journal. 2022; 5(2):210-225.
16. Dako OF, Onalaja TA, Nwachukwu PS, Bankole FA, Lateefat T. Blockchain-enabled systems fostering transparent corporate governance, reducing corruption, and improving global financial accountability. IRE Journals. 2019; 3(3):259-266.
17. Dako OF, Onalaja TA, Nwachukwu PS, Bankole FA, Lateefat T. AI-driven fraud detection enhancing financial auditing efficiency and ensuring improved organizational governance integrity. IRE Journals. 2019; 2(11):556-563.
18. Dako OF, Onalaja TA, Nwachukwu PS, Bankole FA, Lateefat T. Business process intelligence for global enterprises: Optimizing vendor relations with analytical dashboards. IRE Journals. 2019; 2(8):261-270.
19. Davidor S, Dako OF, Nwachukwu PS, Bankole FA, Lateefat T. The post-pandemic leveraged buyout valuation framework for technology sector transactions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(4):773-798. Doi: https://doi.org/10.32628/IJSRCSEIT
20. Davidor S, Dako OF, Nwachukwu PS, Bankole FA, Lateefat T. A predictive stress testing conceptual model for credit covenant breach detection. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(4):680-708. Doi: https://doi.org/10.32628/IJSRCSEIT
21. Didi PU, Abass OS, Balogun O. Strategic Storytelling in Clean Energy Campaigns: Enhancing Stakeholder Engagement Through Narrative Design, 2022.
22. Eboseremen BO, Ogedengbe AO, Obuse E, Oladimeji O, Ajayi JO, Akindemowo AO, *et al*. Secure data integration in multi-tenant cloud environments: Architecture for financial services providers. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):579-592. Doi: https://doi.org/10.54660/.JFMR.2022.3.1.579-592
23. Eboseremen BO, Ogedengbe AO, Obuse E, Oladimeji O, Ajayi JO, Akindemowo AO, *et al*. Developing an AI-driven personalization pipeline for customer retention in investment platforms. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):593-606. Doi: https://doi.org/10.54660/.JFMR.2022.3.1.593-606

24. Essien IA, Cadet E, Ajayi JO, Erigh ED, Obuse E, Ayanbode N, *et al*. Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):618-629. Doi: https://doi.org/10.54660/.JFMR.2022.3.1.618-629
25. Essien IA, Cadet E, Ajayi JO, Erigha ED, Obuse E. Cloud security baseline development using OWASP, CIS benchmarks, and ISO 27001 for regulatory compliance. IRE Journals. 2019; 2(8):250-256. https://irejournals.com/formatedpaper/1710217.pdf
26. Essien IA, Cadet E, Ajayi JO, Erigha ED, Obuse E. Integrated governance, risk, and compliance framework for multi-cloud security and global regulatory alignment. IRE Journals. 2019; 3(3):215-221. https://irejournals.com/formatedpaper/1710218.pdf
27. Etim ED, Essien IA, Ajayi JO, Erigha ED, Obuse E. AI-augmented intrusion detection: Advancements in real-time cyber threat recognition. IRE Journals. 2019; 3(3):225-231. https://irejournals.com/formatedpaper/1710369.pdf
28. Eyinade W, Ezeilo OJ, Ogundeji IA. A Conceptual Model for Evaluating and Strengthening Financial Control Systems in Complex Project Environments, 2022.
29. Eyinade W, Ezeilo OJ, Ogundeji IA. A Framework for Managing Currency Risk and Exchange Rate Exposure in International Energy Investment Portfolios. International Journal of Scientific Research in Civil Engineering. 2022; 6(6):218-230.
30. Eyinade W, Ezeilo OJ, Ogundeji IA. A Stakeholder Engagement Model for Strengthening Transparency in Corporate Financial Performance Reporting, 2022.
31. Eyinade W, Ezeilo OJ, Ogundeji IA. A Value-Based Planning Framework for Linking Financial Forecasts to Business Growth Strategies in the Energy Sector, 2022.
32. Ezeilo OJ, Chima OK, Adesuyi MO. Evaluating the role of trust and transparency in AI-powered retail platforms. Shodhshauryam, International Scientific Refereed Research Journal. 2022; 5(2):226-239.
33. Ezeilo OJ, Chima OK, Ojonugwa BM. AI-augmented forecasting in omnichannel retail: Bridging predictive analytics with customer experience optimization. International Journal of Scientific Research in Science and Technology. 2022; 9(5):1332-1349.
34. Filani OM, Nwokocha GC, Alao OB. Vendor Performance Analytics Dashboard Enabling Real-Time Decision-Making Through Integrated Procurement, Quality, and Cost Metrics, 2022.
35. Filani OM, Olajide JO, Osho GO. A Financial Impact Assessment Model of Logistics Delays on Retail Business Profitability Using SQL, 2022.
36. Filani OM, Olajide JO, Osho GO. A Multivariate Analysis Model for Predicting Sales Performance Based on Inventory and Delivery Metrics, 2022.
37. Ilufoye H, Akinrinoye OV, Okolo CH. A post-crisis retail automation adoption model based on artificial intelligence integration. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(4):579
38. John AO, Oyeyemi BB. The Role of AI in Oil and Gas Supply Chain Optimization. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(1):1075-1086.
39. Kufile OT, Akinrinoye OV, Umezurike SA, Ejike OG, Otokiti BO, Onifade AY. Advances in data-driven decision-making for contract negotiation and supplier selection. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(2):831-842.
40. Kufile OT, Otokiti BO, Onifade AY, Ogunwale B, Harriet C. A framework for integrating social listening data into brand sentiment analytics. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):393-402.
41. Kufile OT, Otokiti BO, Onifade AY, Ogunwale B, Harriet C. Constructing KPI-Driven Reporting Systems for High-Growth Marketing Campaigns. Integration. 2022; 47:p.49.
42. Kufile OT, Otokiti BO, Onifade AY, Ogunwale B, Harriet C. Developing Client Portfolio Management Frameworks for Media Performance Forecasting. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(2):778-788.
43. Kufile OT, Otokiti BO, Onifade AY, Ogunwale B, Harriet C. Building campaign effectiveness dashboards using Tableau for CMO-level decision making. Journal of Frontiers in Multidisciplinary Research. 2022; 3(1):414-424.
44. Kufile OT, Otokiti BO, Onifade AY, Ogunwale B, Okolo CH. Designing retargeting optimization models based on predictive behavioral triggers. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(2):766-777.
45. Mgbame AC, Akpe OE, Abayomi AA, Ogbuefi E, Adeyelu OO, Mgbame AC. Building data-driven resilience in small businesses: A framework for operational intelligence. Iconic Research and Engineering Journals. 2022; 5(9):695-712.
46. Mgbame AC, Akpe OEE, Abayomi AA, Ogbuefi E, Adeyelu OO. Developing low-cost dashboards for business process optimization in SMEs. International Journal of Management and Organizational Research. 2022; 1(1):214-230.
47. Nwokediegwu ZS, Bankole AO, Okiye SE. Advancing interior and exterior construction design through large-scale 3D printing: A comprehensive review. IRE Journals. 2019; 3(1):422-449. ISSN: 2456-8880
48. Nwokediegwu ZS, Bankole AO, Okiye SE. Layered aesthetics: A review of surface texturing and artistic expression in 3D printed architectural interiors. International Journal of Scientific Research in Science and Technology. 2022; 9(6). Doi: https://doi.org/10.32628/IJSRST
49. Nwokocha GC, Alao OB, Filani OM. Multi-Criteria Decision-Making Approach for Sustainable Chemical Supply Chain Design Balancing Safety, Cost, and Environmental Impact, 2022.
50. Odinaka N, Okolo CH, Chima OK, Adeyelu OO. Translating Regulatory Risk into Strategic Opportunity: A Policy-to-Strategy Mapping Toolkit for US Infrastructure Projects, 2022.
51. Ogedengbe AO, Eboseremen BO, Obuse E, Oladimeji O, Ajayi JO, Akindemowo AO, *et al*. Strategic data integration for revenue leakage detection: Lessons from the Nigerian banking sector. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(3):718-728. Doi: https://doi.org/10.54660/.IJMRGE.2022.3.3.718-728

52. Ogedengbe AO, Eboseremen BO, Obuse E, Oladimeji O, Ajayi JO, Akindemowo AO, *et al*. Strategic Data Integration for Revenue Leakage Detection: Lessons from the Nigerian Banking Sector, 2022.
53. Okiye SE, Ohakawa TC, Nwokediegwu ZS. Model for early risk identification to enhance cost and schedule performance in construction projects. IRE Journals. 2022; 5(11). ISSN: 2456-8880
54. Okiye SE, Ohakawa TC, Nwokediegwu ZS. Modeling the integration of Building Information Modeling (BIM) and Cost Estimation Tools to Improve Budget Accuracy in Pre-construction Planning. 2022; 3(2):729-745. ISSN: 2582-7138
55. Okuboye A. Human-in-the-loop automation: Redesigning global business processes to optimize collaboration between AI and employees. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(1):1169-1178. Doi: https://doi.org/10.54660/IJMRGE.2022.3.1.1169-1178
56. Okuboye A. Process agility vs. workforce stability: Balancing continuous improvement with employee well-being in global BPM. International Journal of Multidisciplinary Research and Growth Evaluation. 2022; 3(1):1179-1188. Doi: https://doi.org/10.54660/IJMRGE.2022.3.1.1179-1188
57. Omolayo O, Aduloju TD, Okare BP, Taiwo AE. Digital Twin Frameworks for Simulating Multiscale Patient Physiology in Precision Oncology: A Review of Real-Time Data Assimilation, Predictive Tumor Modeling, and Clinical Decision Interfaces, 2022.
58. Onalaja TA, Nwachukwu PS, Bankole FA, Lateefat T. The environmental, social, and governance cost curve: A conceptual model for quantifying sustainability premiums in emerging markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2022; 8(1):438-445. Doi: https://doi.org/10.32628/IJSRCSEIT
59. Oyeyemi BB. From Warehouse to Wheels: Rethinking Last-Mile Delivery Strategies in the Age of E-commerce, 2022.
60. Ubamadu BC, Bihani D, Daraojimba AI, Osho GO, Omisola JO, Etukudoh EA. Optimizing Smart Contract Development: A Practical Model for Gasless Transactions via Facial Recognition in Blockchain. Int. J. Multidiscip. Res. Growth Eval. 2022; 4(1):978-989.