PROPOSED TITLE System for autonomous verification of compliance with security regulations for cloud-native AI Agents.

The person is *(Recommended that you choose both)*	Applicant // Inventor // **Both**
Title - Dr/Mr/Ms	
First Name	Dinesh
Middle Name	
Surname	Kollu
Residential Address:	9710 Vega Carpio Avenue, NV 89178, Las Vegas
State	Las Vegas
District	
City	
Pin Code	89178
Country of Residence	USA

Bezeichnung: System for autonomous verification of compliance with security regulations for cloud-native AI Agents.

Hauptanspruch: 1. System for autonomous verification of compliance with security regulations for cloud-native AI Agents, comprising:

a monitoring module configured to monitor runtime activities, communication events, infrastructure configurations, and resource utilization associated with one or more cloud-native AI agents operating within distributed cloud computing environments;

a data collection module configured to collect operational information from cloud platforms, orchestration services, application programming interfaces, access control systems, and security management platforms;

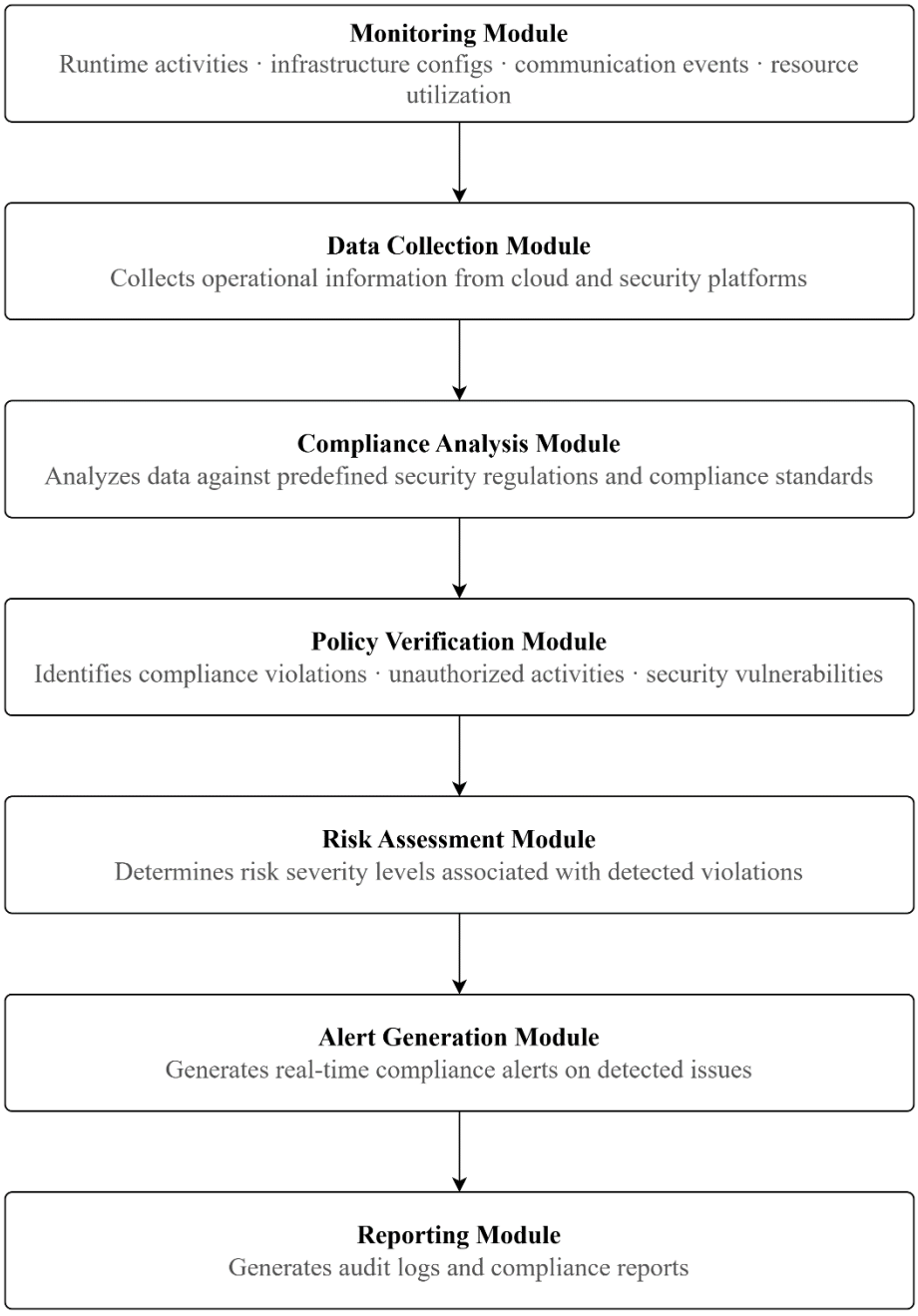
a compliance analysis module configured to analyze the collected operational information based on predefined security regulations, organizational policies, and compliance standards;

a policy verification module configured to identify compliance violations, unauthorized configurations, abnormal behavioral activities, access anomalies, and security vulnerabilities associated with the one or more cloud-native AI agents;

a risk assessment module configured to determine risk severity levels and compliance impact values corresponding to detected violations and anomalies;

an alert generation module configured to generate real-time notifications and compliance breach alerts; and

a reporting module configured to generate audit logs, compliance reports, verification summaries, and regulatory documentation for security governance and compliance management.



[001] The present invention generally relates to cloud computing, cybersecurity, and artificial intelligence technologies. More particularly, the present invention relates to a system for

autonomous verification of compliance with security regulations for cloud-native AI agents operating in distributed computing environments.

[002] Cloud-native AI agents are increasingly deployed across distributed computing environments for automating decision-making, orchestration, monitoring, and service management functions. These AI-driven systems operate within containerized infrastructures, microservices architectures, and hybrid or multi-cloud platforms, where large volumes of sensitive data and critical operational processes are continuously processed. However, existing security compliance verification approaches largely depend on manual audits, static rule-based assessments, and periodic monitoring mechanisms that are unable to efficiently adapt to dynamic cloud-native environments. Conventional systems often fail to provide real-time identification of compliance violations, unauthorized configurations, policy deviations, and evolving security threats associated with autonomous AI agents. Further, regulatory frameworks and organizational security standards require continuous monitoring, verification, and reporting of compliance-related activities. Existing technologies generally lack intelligent autonomous mechanisms capable of correlating runtime behavior, infrastructure configurations, access control policies, and AI agent activities to ensure continuous security regulation compliance across distributed cloud environments. Accordingly, there exists a need for an improved system capable of autonomously verifying compliance with security regulations for cloud-native AI agents through continuous monitoring, intelligent analysis, automated risk detection, and adaptive compliance validation within cloud computing infrastructures.

[003] To solve the problem, the present invention provides a system for autonomous verification of compliance with security regulations for cloud-native AI Agents.

[004] The system enables autonomous verification of compliance with security regulations for cloud-native AI agents operating in distributed cloud environments.

[005] The system performs continuous monitoring of security policies, infrastructure configurations, and operational activities associated with cloud-native AI agents.

[006] The system detects compliance violations, unauthorized access attempts, policy deviations, and security vulnerabilities in real time.

[007] The system analyzes runtime behavior, communication patterns, and resource utilization of cloud-native AI agents for compliance assessment.

[008] The system generates automated compliance reports, audit logs, and risk assessment data for regulatory and organizational review.

[009] The system supports integration with containerized infrastructures, orchestration platforms, and multi-cloud computing environments.

[0010] The system facilitates adaptive verification of evolving security regulations, organizational policies, and compliance standards.

[0011] The system improves operational security, reduces manual auditing efforts, and enhances trustworthiness of autonomous AI-driven cloud services.

[0012] The present invention relates to a system for autonomous verification of compliance with security regulations for cloud-native AI agents operating within distributed cloud computing environments. The system continuously monitors AI agent activities, infrastructure configurations, communication patterns, access control mechanisms, and runtime behaviors across containerized and microservices-based architectures. The system further collects operational data from orchestration platforms, cloud services, application interfaces, and security monitoring modules to identify policy deviations, unauthorized activities, and compliance violations in real time. The system further incorporates intelligent analysis mechanisms for evaluating collected operational data against predefined security regulations, organizational policies, and compliance standards. The system automatically generates compliance reports, audit logs, alerts, and risk assessment outputs to support regulatory verification and security management processes. Additionally, the system supports adaptive integration with hybrid cloud infrastructures, multi-cloud platforms, and dynamically evolving AI-driven environments to improve operational security, reduce manual auditing complexity, and enhance compliance reliability for cloud-native AI agents.

[0013] Fig. 1 illustrates a system architecture for autonomous verification of compliance with security regulations for cloud-native AI agents.

[0014] Fig. 1 illustrates a system architecture for autonomous verification of compliance with security regulations for cloud-native AI agents operating within distributed cloud computing

environments, wherein the architecture includes a monitoring module for monitoring runtime activities, infrastructure configurations, communication events, and resource utilization associated with one or more cloud-native AI agents, a data collection module for collecting operational information from cloud and security platforms, a compliance analysis module for analyzing collected operational data based on predefined security regulations and compliance standards, a policy verification module for identifying compliance violations, unauthorized activities, and security vulnerabilities, a risk assessment module for determining risk severity levels associated with detected violations, an alert generation module for generating real-time compliance alerts and warning notifications, and a reporting module for generating audit logs, compliance reports, verification summaries, and regulatory documentation for continuous security governance and compliance management.

[0015] The present invention discloses a system for autonomous verification of compliance with security regulations for cloud-native AI agents operating within distributed cloud computing environments. The system includes a monitoring module, a data collection module, a compliance analysis module, a policy verification module, a risk assessment module, an alert generation module, and a reporting module interconnected through a communication network. The monitoring module continuously observes runtime activities, infrastructure configurations, communication events, user access operations, and resource utilization associated with cloud-native AI agents deployed across containerized infrastructures, orchestration platforms, and microservices architectures. The monitoring module further verifies that deployed cloud-native AI agents operate within predefined Virtual Private Cloud (VPC) boundaries and comply with network-level security policies associated with the distributed cloud computing environment. The monitoring module continuously analyzes network traffic patterns, access permissions, routing behaviors, and inter-service communications to detect attempts to bypass Network Access Control Lists (NACLs), security groups, firewall rules, or other infrastructure security restrictions. Upon identification of unauthorized network access behavior or policy circumvention attempts, the system generates compliance alerts and risk assessment outputs for maintaining secure operational boundaries of the cloud-native AI agents. The data collection module acquires operational information from cloud platforms, application programming interfaces, security management systems, orchestration services, access control mechanisms, and infrastructure monitoring tools. The compliance analysis module evaluates the collected operational information against

predefined security regulations, organizational policies, governance standards, and compliance rules. The policy verification module identifies unauthorized configurations, policy deviations, abnormal behavioral patterns, access anomalies, and potential security vulnerabilities associated with the cloud-native AI agents. The risk assessment module further determines risk severity levels and compliance impact scores based on detected violations and operational anomalies. The alert generation module produces real-time notifications, warning signals, and compliance breach alerts for system administrators, security operators, or external monitoring entities. The reporting module automatically generates audit logs, compliance reports, verification summaries, and regulatory documentation for security review and governance purposes. The system further supports adaptive integration with hybrid cloud infrastructures, multi-cloud computing environments, and dynamically scalable AI-driven platforms to enable continuous compliance verification, automated security assessment, and improved operational reliability for cloud-native AI agents.

We Claim,

1. System for autonomous verification of compliance with security regulations for cloud-native AI Agents, comprising:

a monitoring module configured to monitor runtime activities, communication events, infrastructure configurations, and resource utilization associated with one or more cloud-native AI agents operating within distributed cloud computing environments;

a data collection module configured to collect operational information from cloud platforms, orchestration services, application programming interfaces, access control systems, and security management platforms;

a compliance analysis module configured to analyze the collected operational information based on predefined security regulations, organizational policies, and compliance standards;

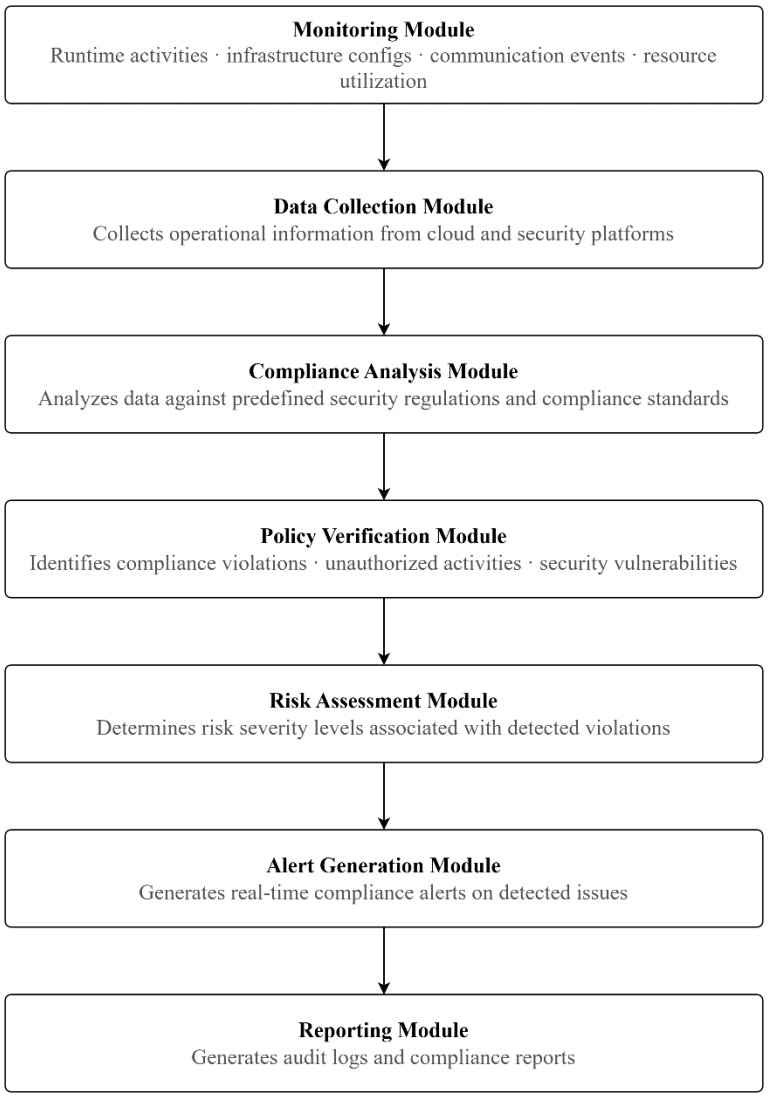
a policy verification module configured to identify compliance violations, unauthorized configurations, abnormal behavioral activities, access anomalies, and security vulnerabilities associated with the one or more cloud-native AI agents;

a risk assessment module configured to determine risk severity levels and compliance impact values corresponding to detected violations and anomalies;

an alert generation module configured to generate real-time notifications and compliance breach alerts; and

a reporting module configured to generate audit logs, compliance reports, verification summaries, and regulatory documentation for security governance and compliance management.

2. The system as claimed in claim 1, wherein the monitoring module continuously tracks operational activities of containerized AI agents deployed within microservices-based architectures.
3. The system as claimed in claim 1, wherein the data collection module acquires operational data from hybrid cloud infrastructures and multi-cloud computing environments.
4. The system as claimed in claim 1, wherein the compliance analysis module compares operational information with predefined regulatory policies to determine compliance status.
5. The system as claimed in claim 1, wherein the policy verification module detects unauthorized access attempts, policy deviations, and abnormal communication patterns.
6. The system as claimed in claim 1, wherein the risk assessment module assigns compliance risk scores based on severity levels associated with identified violations.
7. The system as claimed in claim 1, wherein the alert generation module transmits automated warning notifications to system administrators upon detection of compliance breaches.
8. The system as claimed in claim 1, wherein the reporting module generates downloadable compliance verification reports and audit documentation.
9. The system as claimed in claim 1, wherein the system supports adaptive integration with orchestration platforms including Kubernetes-based environments.
10. The system as claimed in claim 1, wherein the monitoring module verifies that the one or more cloud-native AI agents operate within predefined Virtual Private Cloud (VPC) boundaries and prevents bypassing of Network Access Control Lists (NACLs) and security group policies


Monitoring Module
Runtime activities · infrastructure configs · communication events · resource utilization
Data Collection Module
Collects operational information from cloud and security platforms
Compliance Analysis Module
Analyzes data against predefined security regulations and compliance standards
Policy Verification Module
Identifies compliance violations · unauthorized activities · security vulnerabilities
Risk Assessment Module
Determines risk severity levels associated with detected violations
Alert Generation Module
Generates real-time compliance alerts on detected issues
Reporting Module
Generates audit logs and compliance reports