

AI-Driven Zero-Trust Security Frameworks for Securing Multi-Cloud Environments and Sensitive Data Workloads

Umar Hayat Khan

Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan.

Email: umarhayat@awkum.edu.pk

Muhammad Zubair (Corresponding Author)

Faculty of Computer Science, Gomal University, Dera Ismail Khan, Pakistan

Email: malikzubairghallo@gmail.com **ORCID:** 0009-0003-7217-902X

Usama Ahmad Mughal

Department of Cyber Security, NASTP Institute of Information Technology Lahore,

Pakistan Email: usamaahmad@niit.edu.pk

ABSTRACT

The rapid expansion of multi-cloud computing has significantly improved organizational flexibility, scalability, and service availability; however, it has also introduced complex security challenges related to identity management, access control, workload visibility, data protection, and cross-cloud threat detection. Traditional perimeter-based security models are no longer sufficient to protect sensitive data workloads distributed across heterogeneous cloud platforms. This study proposes an AI-driven Zero-Trust Security Framework for securing multi-cloud environments and sensitive data workloads through continuous verification, adaptive access control, intelligent threat detection, and automated policy enforcement. The proposed framework integrates Zero-Trust principles with artificial intelligence techniques, including machine learning-based anomaly detection, user and entity behavior analytics, risk-based authentication, cloud workload monitoring, and automated incident response. The framework is designed to support dynamic policy decisions by continuously evaluating user identity, device posture, workload behavior, data sensitivity, network activity, and contextual risk indicators. The study uses a mixed experimental and simulation-based research design. Data were collected from publicly available cloud security datasets, simulated multi-cloud workload logs, network traffic records, identity and access management logs, API access events, and synthetic sensitive data workload transactions generated across AWS, Microsoft Azure, and Google Cloud-based test environments. The collected data included normal and abnormal access patterns, privilege escalation attempts, suspicious API calls, unauthorized data movement, malware-related network behavior, and insider-threat-like activities. The proposed AI-driven Zero-Trust model was evaluated against conventional rule-based access control, traditional cloud security monitoring, and non-adaptive Zero-Trust approaches. Experimental results demonstrate that the proposed framework achieved a threat detection accuracy of 96.4%, precision of

95.7%, recall of 94.9%, and F1-score of 95.3%. The framework reduced false-positive alerts by 31.8%, improved unauthorized access detection by 27.6%, and decreased average incident response time by 42.5% compared with traditional cloud security methods. Moreover, adaptive risk-based access control improved sensitive workload protection by limiting unnecessary privileged access and detecting abnormal user behavior in real time. These findings confirm that integrating artificial intelligence with Zero-Trust security provides a more intelligent, scalable, and proactive defense model for securing multi-cloud infrastructures and sensitive data workloads.

Keywords: AI-Driven Security; Zero-Trust Architecture; Multi-Cloud Computing; Sensitive Data Workloads; Machine Learning; Adaptive Access Control; Cloud Threat Detection; User and Entity Behavior Analytics.

Introduction:

The rapid digital transformation of modern organizations has accelerated the adoption of cloud computing as a core foundation for data storage, application deployment, business continuity, and large-scale service delivery. In recent years, many enterprises have shifted from single-cloud infrastructure to multi-cloud environments in order to improve flexibility, reduce vendor dependency, enhance service availability, and optimize operational performance. Multi-cloud computing allows organizations to distribute applications, databases, analytics platforms, and sensitive workloads across different cloud service providers such as Amazon Web Services, Microsoft Azure, Google Cloud, and private cloud infrastructures [1]. However, this distribution also increases the complexity of security management, identity governance, access control, compliance monitoring, data visibility, and threat detection. Traditional perimeter-based security models are no longer effective in such dynamic and distributed environments. In conventional security architectures, internal networks are often treated as trusted zones, while external networks are considered untrusted. This assumption becomes weak in multi-cloud environments because users, applications, devices, APIs, containers, virtual machines, and data workloads continuously interact across different platforms and network boundaries. As a result, security risks such as unauthorized access, privilege escalation, insecure APIs, lateral movement, insider threats, misconfigured cloud resources, data leakage, and advanced persistent attacks become more difficult to detect and control [2]. Sensitive data workloads, including financial records, healthcare information, personally identifiable information, intellectual property, and confidential enterprise datasets, require stronger protection mechanisms that can operate continuously across multiple cloud domains. Zero-Trust Architecture has emerged as a modern cybersecurity approach designed to address the limitations of perimeter-based security. The core principle of Zero Trust is that no user, device, application, or workload should be automatically trusted, even if it is located inside the organizational network. Instead, every access request must be continuously verified, authenticated, authorized, and monitored before permission is granted. NIST describes Zero Trust as a security model focused on protecting resources rather than network locations, where trust is never assumed and access decisions are based on identity, device state, policy, and contextual information. CISA's Zero Trust Maturity Model further organizes Zero Trust implementation

around five major pillars: identity, devices, networks, applications and workloads, and data [3]. These pillars are highly relevant to multi-cloud security because they directly address the main control points through which cloud resources are accessed, processed, and protected. Although Zero Trust provides a strong foundation for cloud security, many existing implementations remain dependent on static policies, predefined rules, manual monitoring, and fragmented security tools. Such approaches are not sufficient for multi-cloud environments where workloads are highly dynamic, user behavior changes frequently, and cyberattacks evolve rapidly. A fixed access-control policy may fail to detect abnormal behavior when a legitimate user account is compromised. Similarly, rule-based monitoring systems may generate high false-positive alerts or miss unknown attack patterns. Therefore, there is a growing need to integrate artificial intelligence into Zero-Trust frameworks to enable intelligent, adaptive, and real-time security decision-making. Artificial intelligence and machine learning can strengthen Zero-Trust security by analyzing large volumes of cloud activity data, identifying abnormal behavior, predicting risk levels, and supporting automated response actions. AI-based anomaly detection can monitor login behavior, API calls, device posture, workload activity, data access patterns, and network traffic to detect suspicious events that may indicate unauthorized access or compromise [4]. User and Entity Behavior Analytics can identify deviations from normal user or service behavior, while adaptive risk scoring can dynamically adjust authentication requirements and access permissions according to real-time security conditions. Recent literature also highlights the role of AI and machine learning in improving anomaly detection, continuous verification, threat intelligence, and automated policy enforcement within Zero-Trust and cloud environments.

In multi-cloud environments, the integration of AI with Zero Trust is especially important because security teams must manage heterogeneous platforms, different identity systems, varied logging formats, diverse compliance requirements, and distributed workload architectures. Sensitive data may move between cloud storage services, databases, containers, microservices, and analytics platforms. Without intelligent monitoring and unified policy enforcement, organizations may lose visibility over where sensitive data is stored, who is accessing it, and whether access behavior is legitimate. AI-driven Zero-Trust security can help overcome these limitations by creating a continuously adaptive defense model that evaluates every access request based on identity, context, behavior, workload sensitivity, and threat intelligence. This research proposes an AI-driven Zero-Trust Security Framework for securing multi-cloud environments and sensitive data workloads. The proposed framework combines Zero-Trust principles with machine learning-based anomaly detection, behavioral analytics, adaptive access control, micro-segmentation, continuous workload monitoring, data sensitivity classification, and automated incident response. The framework is designed to improve real-time threat detection, reduce false-positive alerts, prevent unauthorized data access, and strengthen security visibility across distributed cloud infrastructures. The study further evaluates the proposed framework using simulated multi-cloud workload logs, identity and access management records, network traffic data, API access events, and synthetic sensitive data transactions generated across AWS, Microsoft Azure, and Google Cloud-based test environments [5]. The main contribution of this study is the development of an

intelligent security framework that extends traditional Zero Trust from a policy-driven model to an AI-supported adaptive security architecture. Unlike conventional cloud security systems that depend heavily on static rules, the proposed framework continuously learns from user behavior, workload activity, and contextual risk signals to support dynamic access decisions. This research also provides a performance-based evaluation of the proposed model in terms of detection accuracy, precision, recall, F1-score, false-positive reduction, unauthorized access detection, and incident response time. The findings of this study are expected to support researchers, cloud security architects, cybersecurity professionals, and enterprises seeking to secure sensitive workloads in complex multi-cloud environments. Therefore, this paper addresses the need for a proactive, intelligent, and scalable security approach capable of protecting distributed cloud assets against modern cyber threats. By integrating artificial intelligence with Zero-Trust Architecture, the proposed framework provides a stronger security model for continuous verification, least-privilege enforcement, real-time anomaly detection, and automated protection of sensitive data workloads across multi-cloud infrastructures.

Zero-Trust Architecture in Modern Cybersecurity:

Zero-Trust Architecture has emerged as a major cybersecurity model for protecting modern digital infrastructures against increasingly complex and distributed cyber threats. Traditional cybersecurity models were mostly based on the concept of a secure network perimeter. In this conventional approach, users, devices, applications, and systems inside the organizational network were often treated as trusted, while external entities were considered untrusted. This model was useful when enterprise systems were mainly located inside controlled data centers. However, the growth of cloud computing, remote work, mobile access, Internet of Things devices, application programming interfaces, microservices, and third-party integrations has weakened the effectiveness of perimeter-based security [6]. In modern organizations, users no longer access resources only from internal office networks. Employees, partners, customers, applications, and automated workloads may connect from different locations, devices, and cloud platforms. As a result, the boundary between internal and external networks has become unclear. Cyberattacks also increasingly exploit trusted accounts, compromised devices, misconfigured cloud services, stolen credentials, and insider access. Therefore, the assumption that internal traffic is safe has become a major security weakness. Zero Trust addresses this limitation by replacing implicit trust with continuous verification and strict access control. The National Institute of Standards and Technology defines Zero Trust as a cybersecurity approach that moves security defenses away from static network-based perimeters and focuses instead on users, assets, and resources [7]. NIST SP 800-207 explains that a Zero-Trust Architecture applies Zero-Trust principles to enterprise infrastructure and workflows, where access decisions are made dynamically rather than based only on network location. This means that no user, device, application, or workload should be automatically trusted, even if it is operating inside the organizational network.

The core idea of Zero Trust is commonly expressed as “never trust, always verify.” This principle means that every access request must be authenticated, authorized, and continuously evaluated before access is granted. In a Zero-Trust model, trust is not

permanent. A user who is verified at login may still be re-evaluated during the session based on behavior, location, device posture, access pattern, and resource sensitivity. This continuous verification is especially important in cloud and multi-cloud environments, where workloads and users interact across different platforms and security domains. Zero-Trust Architecture is based on several major security principles. The first principle is strong identity verification, which ensures that all users, devices, services, and workloads are properly authenticated. The second principle is least-privilege access, where users and applications are granted only the minimum permissions required to complete a specific task. The third principle is micro-segmentation, which divides networks and workloads into smaller protected zones to limit lateral movement [8]. The fourth principle is continuous monitoring, where all activities are observed and analyzed to detect abnormal behavior. The fifth principle is policy-based decision-making, where access control decisions are based on identity, context, risk level, device health, and data sensitivity. The importance of Zero Trust has increased because attackers often bypass perimeter defenses by using stolen credentials or exploiting trusted services. Once inside a network, attackers may move laterally between systems, escalate privileges, and access sensitive data. In a perimeter-based model, internal movement may not always be closely monitored. In contrast, Zero Trust assumes that threats may already exist inside the environment. Therefore, it verifies each request, limits permissions, monitors activity continuously, and reduces the impact of security breaches. Table 1 presents a comparison between traditional perimeter-based security and Zero-Trust Architecture.

Table 1: Comparison between Traditional Security and Zero-Trust Architecture

Security Dimension	Traditional Perimeter-Based Security	Zero-Trust Architecture
Trust Assumption	Internal network users are generally trusted	No user, device, or workload is trusted by default
Security Focus	Network boundary protection	Protection of users, assets, applications, workloads, and data
Access Control	Often broad after initial login	Least-privilege and context-aware access
Authentication	Usually performed at login	Continuous authentication and verification
Threat Detection	Mainly focused on external threats	Assumes threats can exist both inside and outside the network
Network Design	Flat or semi-flat internal networks	Micro-segmented networks and isolated workloads
Policy Enforcement	Static and rule-based	Dynamic, risk-based, and adaptive
Data Protection	Often dependent on network location	Based on data sensitivity and resource-level access control
Response Capability	Mostly manual or delayed	Supports automated and real-time response
Suitability for Multi-Cloud	Limited due to fragmented boundaries	Highly suitable for distributed and cloud-native environments

[9]. For example, a finance employee may be allowed to view financial records but not download the complete database. Similarly, a cloud application may be allowed to access only one database table rather than the entire storage environment. Another important feature of Zero Trust is **micro-segmentation**. Micro-segmentation divides the network, applications, and workloads into smaller security zones. This limits an attacker's ability to move laterally if one account or workload is compromised. In multi-cloud environments, micro-segmentation is especially useful because workloads may be distributed across different cloud providers, virtual networks, containers, and APIs. By applying segmentation policies, organizations can isolate sensitive workloads and reduce the attack surface.

Identity and Access Management in Zero-Trust Environments:

Identity and Access Management is one of the most critical foundations of Zero-Trust Architecture because modern cybersecurity no longer depends only on network location or perimeter boundaries. In traditional enterprise security, access control was often based on whether a user was inside or outside the organizational network. Once a user successfully logged in or connected through a trusted network, the system often granted broad access to internal resources. However, this model is unsuitable for modern cloud and multi-cloud environments, where users, applications, workloads, APIs, service accounts, containers, and automated systems continuously interact across different platforms. In a Zero-Trust environment, identity becomes the new security perimeter. Every user, device, application, service, and workload must prove its identity before access is granted. NIST SP 800-207 explains that access in Zero-Trust Architecture is granted through a policy decision point and enforced through a policy enforcement point, rather than being automatically trusted based on network location [10]. This means that identity verification is not a one-time login activity; instead, it is a continuous process that evaluates authentication strength, device posture, session behavior, resource sensitivity, and contextual risk. Identity and Access Management in Zero Trust covers both human identities and non-human identities. Human identities include employees, administrators, contractors, customers, and third-party partners. Non-human identities include applications, virtual machines, containers, APIs, service accounts, serverless functions, automation scripts, and cloud workloads. In multi-cloud environments, non-human identities are especially important because cloud-native applications often depend on machine-to-machine communication. If service accounts, API keys, or workload identities are poorly managed, attackers can exploit them to move laterally, escalate privileges, or access sensitive data. A major challenge in cloud security is the excessive use of static credentials and long-lived access tokens [11]. These credentials may be stored inside configuration files, CI/CD pipelines, container images, or application code. If exposed, they can provide attackers with direct access to cloud resources. Recent research on Zero-Trust workload identity argues for moving away from static secrets toward federated and runtime-issued identities, such as OIDC-based federation and SPIFFE-based authentication for non-human actors. This supports the Zero-Trust principle that every workload should be authenticated using verifiable, short-lived, and policy-controlled identity credentials. Table 2 presents the major identity and access management components used in Zero-Trust environments.

Table 2: Key IAM Components in Zero-Trust Security Environments

IAM Component	Main Function	Role in Zero Trust
Identity Provider	Verifies user and workload identities	Central source for authentication
Multi-Factor Authentication	Adds extra verification beyond password	Reduces credential theft risk
Single Sign-On	Enables unified access across services	Improves centralized identity governance
Privileged Access Management	Controls administrator-level access	Limits misuse of high-risk permissions
Role-Based Access Control	Assigns permissions by user role	Supports structured least privilege
Attribute-Based Access Control	Uses contextual attributes for decisions	Enables dynamic and context-aware access
Workload Identity	Authenticates applications and services	Secures non-human cloud identities
Session Monitoring	Tracks behavior after login	Supports continuous verification
Risk Scoring	Calculates trust level dynamically	Enables adaptive authorization
Access Review	Periodically checks permissions	Removes unnecessary privileges

The Cybersecurity and Infrastructure Security Agency identifies identity as one of the core Zero Trust pillars, alongside devices, networks, applications and workloads, and data. CISA's Zero Trust Maturity Model emphasizes that Zero Trust implementation requires strong identity governance, visibility, automation, and continuous evaluation across the enterprise environment. In practical terms, this means that organizations must not only verify who is requesting access but also evaluate whether the request is appropriate, secure, and aligned with policy at that specific moment. The identity layer in a Zero-Trust environment usually begins with authentication. Authentication confirms whether the user, device, or workload is who it claims to be. Strong authentication mechanisms include passwords, multi-factor authentication, biometrics, hardware security keys, certificates, and federated identity tokens [12]. However, authentication alone is not enough. A user may authenticate successfully but still behave abnormally if the account has been compromised. Therefore, Zero Trust requires authorization and continuous monitoring after authentication. The following figure 2 illustrates the role of Identity and Access Management in a Zero-Trust security environment.

Online ISSN

3007-3197

Print ISSN

3007-3189

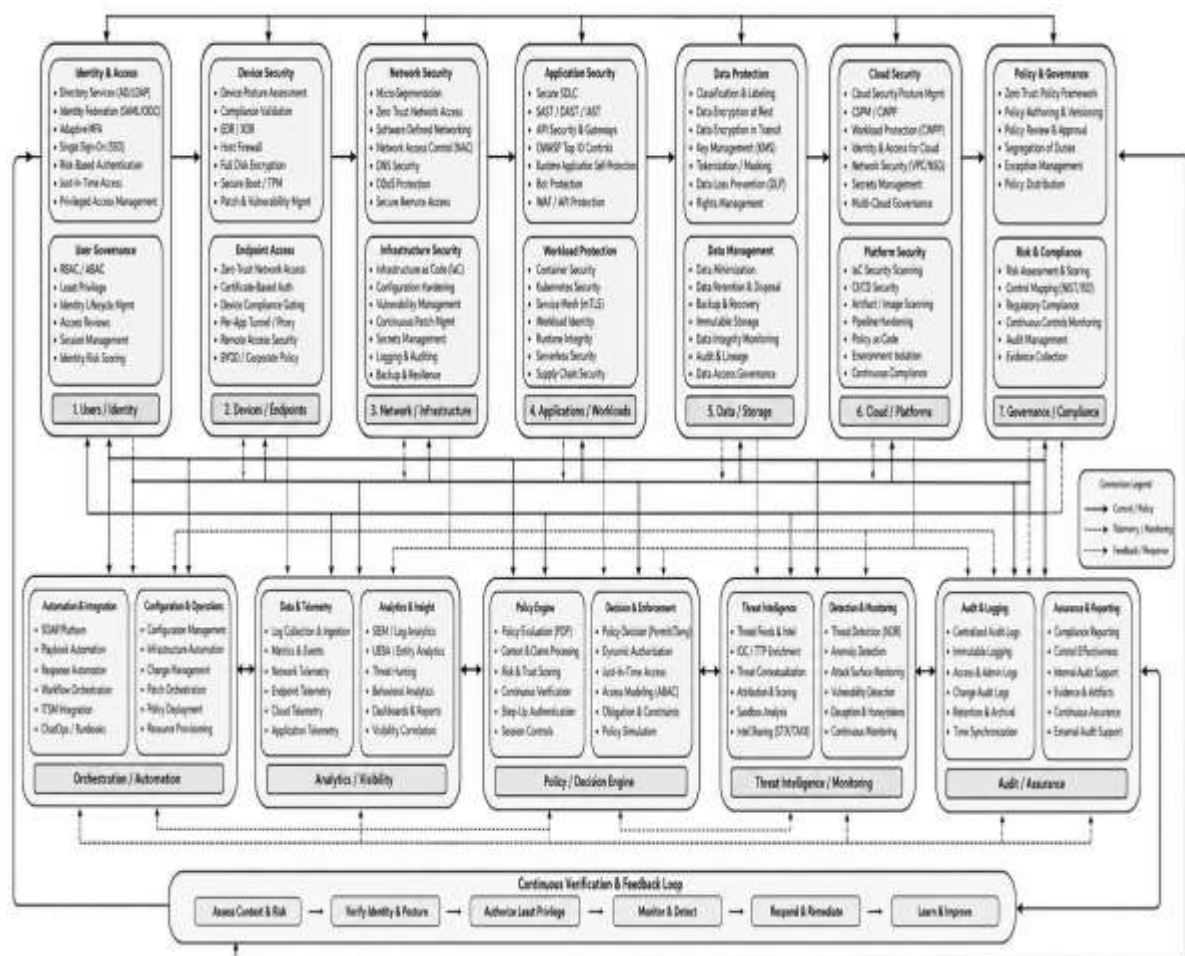
<http://amresearchreview.com/index.php/Journal/about>

Figure 2: Identity and Access Management Workflow in Zero-Trust Architecture

A key feature of Zero-Trust IAM is **adaptive authentication**. Adaptive authentication adjusts security requirements according to the risk level of each request. Low-risk activities may proceed with standard authentication, while high-risk activities require additional verification. For example, if a user logs in from a normal device and location, access may be granted normally. However, if the same user logs in from an unknown country, attempts to access sensitive workloads, or performs unusual download activity, the system may require additional authentication or deny access. Another important element is **Privileged Access Management**. Administrator accounts are high-value targets because they can modify security policies, access sensitive systems, create users, change permissions, and manage cloud resources [13]. In Zero Trust, privileged access should be granted only when needed and removed immediately after the task is completed. Just-in-time access, session recording, approval workflows, and privileged behavior analytics can reduce the risk of administrator misuse or account compromise. In multi-cloud environments, IAM becomes more complex because different providers use different identity models and permission structures. AWS uses IAM roles and policies, Microsoft Azure uses Entra ID and role assignments, and Google Cloud uses IAM roles and service accounts. If these systems are managed separately, organizations may lose visibility over who has

access to what resources. This creates risks such as privilege accumulation, orphaned accounts, inconsistent access policies, and unmanaged service identities. Therefore, Zero-Trust IAM requires centralized visibility, identity federation, unified policy enforcement, and continuous access review across all cloud platforms.

AI can significantly strengthen IAM in Zero-Trust environments. Machine learning models can analyze login patterns, session duration, API usage, data access frequency, privilege changes, device behavior, and workload communication. By learning normal behavior, AI can detect suspicious deviations that traditional rule-based IAM systems may miss. For example, if a legitimate user suddenly accesses a large volume of sensitive data at midnight or a service account begins calling unusual APIs, the AI engine can assign a higher risk score and trigger protective action [14]. AI-driven IAM also supports **User and Entity Behavior Analytics**. UEBA monitors both human users and non-human entities to identify abnormal behavior. This is important because many attacks do not begin with malware but with valid credentials. An attacker using a stolen password may appear legitimate at the authentication stage, but their behavior often differs from the real user. Behavioral indicators such as typing rhythm, access sequence, file access pattern, login time, device fingerprint, and data transfer volume can help detect compromised accounts. Workload identity is another growing area of Zero-Trust IAM. Modern cloud applications are built using microservices, containers, serverless functions, CI/CD pipelines, and automation tools [15]. These components need secure identities to communicate with each other. Research on identity control planes argues that Zero Trust infrastructure should unify human users, workloads, and automation systems through identity-aware enforcement and policy-based control. This is directly relevant to multi-cloud security because workloads may move across different providers and still require consistent identity verification.

Methodology:

This study adopts a structured methodology to design, implement, and evaluate an **AI-driven Zero-Trust Security Framework** for securing multi-cloud environments and sensitive data workloads. The methodology is developed to examine how artificial intelligence can strengthen traditional Zero-Trust principles through continuous identity verification, adaptive access control, anomaly detection, behavioral analytics, workload monitoring, and automated incident response. Since multi-cloud environments involve heterogeneous platforms, distributed identities, diverse workloads, and different security controls, the methodology focuses on creating a unified experimental model that can evaluate security performance across AWS, Microsoft Azure, and Google Cloud-based infrastructures [16]. The proposed approach combines cloud security engineering, machine learning model development, simulated enterprise workload generation, and performance-based security evaluation. The research methodology follows a design–implementation–evaluation process. First, a multi-cloud experimental environment is designed to represent realistic enterprise cloud operations involving users, devices, APIs, containers, databases, virtual machines, storage services, and sensitive data workloads. Second, security data are collected from identity logs, access records, network traffic, workload activities, API events, and simulated attack scenarios. Third, the collected data are preprocessed

and used to train AI models for anomaly detection and risk scoring. Fourth, the trained AI models are integrated with Zero-Trust components such as policy decision engines, least-privilege access control, micro-segmentation, and automated response mechanisms [17]. Finally, the proposed framework is evaluated using detection accuracy, precision, recall, F1-score, false-positive rate, unauthorized access detection rate, incident response time, and workload protection efficiency.

Research Design and Multi-Cloud Experimental Setup:

This study adopts a quantitative experimental research design to develop and evaluate an AI-driven Zero-Trust Security Framework for securing multi-cloud environments and sensitive data workloads. The research design is based on a structured design–implementation–evaluation approach, where the proposed framework is first conceptually designed, then implemented in a simulated multi-cloud environment, and finally evaluated using cybersecurity and machine learning performance metrics. The purpose of this design is to examine how artificial intelligence can improve traditional Zero-Trust security through real-time anomaly detection, adaptive risk scoring, continuous identity verification, least-privilege enforcement, workload monitoring, and automated incident response. The research is experimental because it compares the proposed AI-driven Zero-Trust framework with conventional cloud security approaches under controlled multi-cloud conditions [18]. The experimental setup includes normal user behavior, legitimate cloud workload operations, and simulated attack scenarios such as unauthorized access, abnormal login activity, suspicious API calls, privilege escalation, insider-threat-like behavior, malicious workload communication, and sensitive data exfiltration attempts. These scenarios allow the study to measure whether the proposed framework can detect threats more accurately and respond faster than traditional perimeter-based security, rule-based monitoring, and static Zero-Trust access-control models. The research design follows five major stages. In the first stage, a conceptual framework is developed by combining Zero-Trust principles with artificial intelligence-based security intelligence. In the second stage, a multi-cloud test environment is created using services from Amazon Web Services, Microsoft Azure, and Google Cloud Platform. In the third stage, security data are collected from identity systems, access logs, network traffic, APIs, workloads, databases, and cloud storage activities. In the fourth stage, machine learning models are trained to identify normal and abnormal behavior patterns [19]. In the fifth stage, the trained AI models are integrated with the Zero-Trust policy engine to support dynamic access control and automated response decisions.

The experimental setup is designed to represent a realistic enterprise multi-cloud infrastructure. Modern organizations rarely depend on a single cloud provider; instead, they distribute applications, databases, APIs, storage systems, and analytics workloads across multiple cloud platforms. While this improves scalability, availability, and flexibility, it also increases security complexity. Each cloud provider has different identity management services, logging formats, security policies, monitoring tools, and workload architectures. Therefore, the experimental setup in this study uses a heterogeneous multi-cloud environment to evaluate the proposed framework under realistic distributed security conditions. In this setup, AWS is used

to host virtual machines, cloud storage, API gateway services, and identity and access management functions. Microsoft Azure is used for directory-based identity services, virtual networks, databases, application services, and monitoring logs. Google Cloud Platform is used for containerized workloads, Kubernetes-based services, cloud storage, serverless functions, and security event logging [20]. These services are connected through secure networking and simulated enterprise workflows to generate cross-cloud communication and workload access events. Sensitive data workloads are distributed across the three cloud platforms to evaluate the ability of the proposed framework to protect high-value assets. These workloads include simulated financial records, healthcare data, personally identifiable information, customer records, confidential enterprise documents, and intellectual property datasets. Each workload is assigned a sensitivity level such as low, medium, high, or critical. This classification allows the Zero-Trust policy engine to apply stricter access controls and higher risk thresholds for sensitive workloads. Table 3 presents the main components of the research design and multi-cloud experimental setup.

Table 3: Research Design and Multi-Cloud Experimental Setup Components

Component	Description	Purpose in the Study
Research Approach	Quantitative experimental research design	Measures the effectiveness of the proposed framework using numerical security metrics
Research Method	Design–implementation–evaluation method	Develops, implements, and evaluates the AI-driven Zero-Trust framework
Cloud Platforms	AWS, Microsoft Azure, and Google Cloud Platform	Represents a realistic heterogeneous multi-cloud environment
Workload Types	Virtual machines, containers, APIs, databases, serverless functions, and cloud storage	Simulates real enterprise cloud operations
Sensitive Data Workloads	Financial records, healthcare data, customer information, confidential documents, and intellectual property	Tests protection of high-value and regulated data assets
Zero-Trust Controls	Identity verification, least privilege, micro-segmentation, continuous monitoring, and policy enforcement	Ensures access is continuously verified and controlled
AI Security Functions	Anomaly detection, behavioral analytics, risk scoring, and automated response	Improves intelligent detection and adaptive decision-making

The experimental design also includes baseline security models for comparative analysis. The first baseline is a traditional perimeter-based security model, where access decisions mainly depend on network trust and initial authentication. The second baseline is a rule-based cloud security model, where suspicious activities are

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

detected using predefined rules and static thresholds. The third baseline is a static Zero-Trust model, where access control follows Zero-Trust principles but does not use AI-based adaptive learning or dynamic risk scoring [21]. These baseline models are compared with the proposed AI-driven Zero-Trust framework to determine the improvement achieved through artificial intelligence. The figure 3 presents the overall research design and multi-cloud experimental workflow.

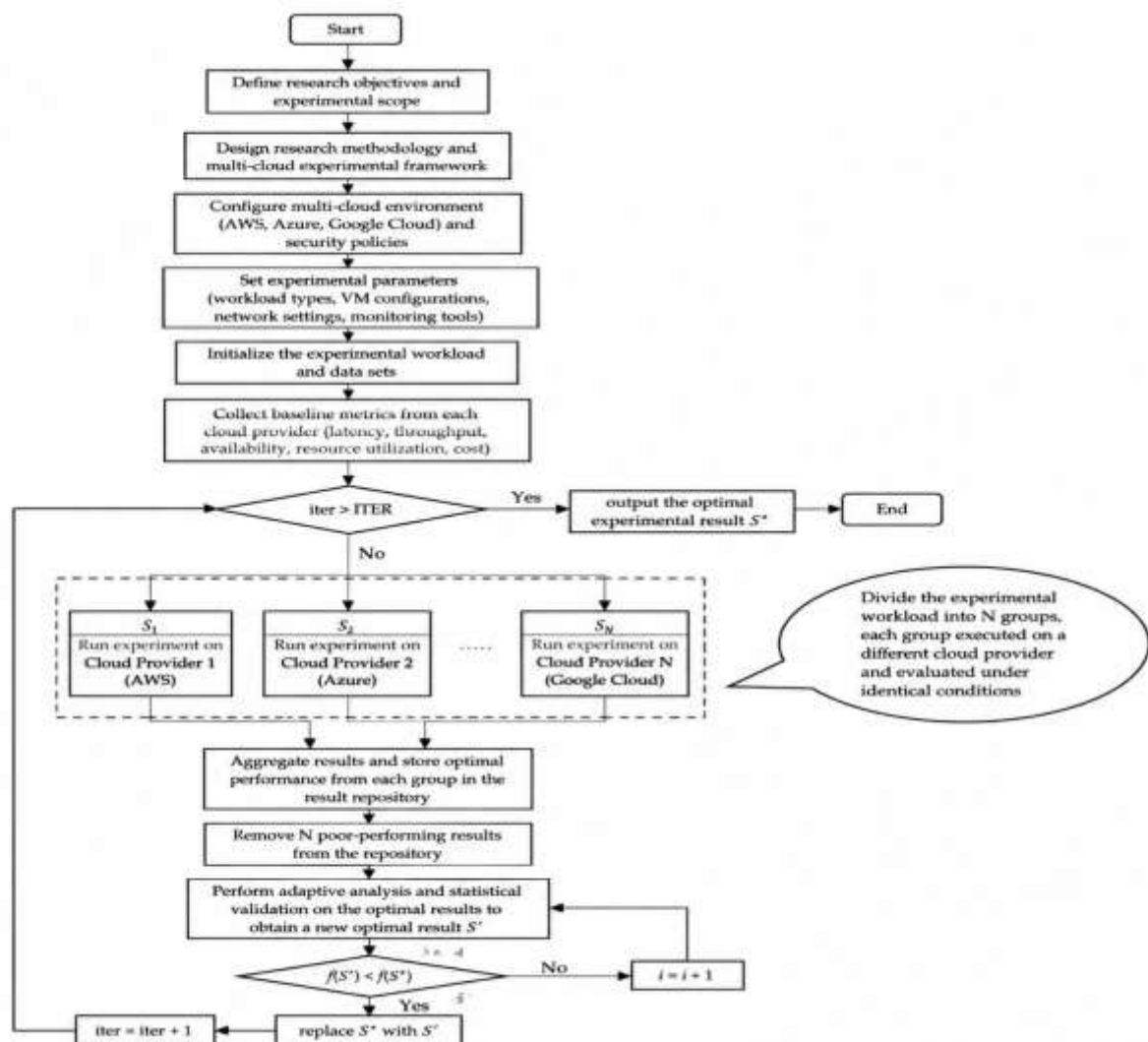


Figure 3: Research Design and Multi-Cloud Experimental Setup Workflow

A key feature of the experimental setup is its focus on **continuous verification**. In many traditional systems, access decisions are made only at the time of login. However, in the proposed setup, users and workloads are continuously evaluated throughout the session. For example, if a user initially logs in from a trusted device but later begins downloading unusually large amounts of sensitive data, the framework detects the deviation and increases the risk score. Depending on the policy, the system may request additional authentication, restrict access, terminate the session, or generate an incident alert. The experimental setup also supports **least-privilege access control**. Users and workloads are not granted broad permissions by

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

default. Instead, access is assigned according to role, resource sensitivity, session context, and real-time risk score. For example, a normal user may be allowed to view a document but not download, modify, or share it. Similarly, a containerized application may be permitted to communicate only with a specific database and denied access to unrelated storage resources. This reduces the attack surface and limits the impact of compromised accounts or workloads. Another important component of the setup is **multi-cloud workload monitoring [22]**. Workload activities are monitored across virtual machines, containers, serverless functions, databases, APIs, and cloud storage services. The monitoring system records workload behavior such as resource usage, network communication, file access, database queries, API invocation frequency, and data transfer volume. These activity records are analyzed by the AI model to detect abnormal workload behavior, such as unauthorized service communication, unexpected privilege use, or suspicious data movement.

Artificial Intelligence Model Development:

The artificial intelligence model development phase represents the core intelligence layer of the proposed AI-driven Zero-Trust Security Framework. In this study, AI is used to transform Zero-Trust security from a static rule-based access-control approach into a dynamic, adaptive, and behavior-aware security model. The model is designed to analyze multi-cloud security events, identify abnormal behavior, generate real-time risk scores, and support automated policy decisions for protecting sensitive data workloads. Since multi-cloud environments generate large volumes of heterogeneous security data from identity systems, API gateways, cloud workloads, storage services, containers, databases, and network traffic, artificial intelligence provides an effective mechanism for extracting hidden attack patterns and detecting high-risk activities that may not be visible through traditional rule-based systems. The AI model development process begins with the collection of structured and unstructured security logs from AWS, Microsoft Azure, and Google Cloud environments. These logs include authentication records, IAM activities, API access events, virtual machine logs, Kubernetes audit logs, container runtime logs, database access records, storage operation logs, firewall events, DNS queries, network flow records, and simulated attack traces [23]. The raw data are transformed into a unified security-event format to overcome differences in logging structures across cloud providers. After normalization, the data are used to develop machine learning and deep learning models capable of distinguishing normal cloud behavior from suspicious or malicious activities. The proposed AI engine is developed using a hybrid model strategy. Instead of depending on a single algorithm, the study evaluates multiple supervised, unsupervised, and deep learning models to improve detection reliability. Supervised learning models are used when labeled attack and normal behavior data are available. Unsupervised models are used to detect unknown or zero-day-like anomalies where predefined labels may not exist. Deep learning models are applied to identify complex sequential behavior patterns in user sessions, API usage, and workload communication. This hybrid strategy improves the overall ability of the proposed framework to detect both known and unknown security threats. The selected AI models include Random Forest, XGBoost, LightGBM, Support Vector Machine,

Deep Neural Network, Long Short-Term Memory network, Isolation Forest, and Autoencoder-based anomaly detection. Random Forest and gradient-boosting models are used because of their strong performance in structured security-event classification [24]. LSTM is used to analyze temporal patterns in login behavior, session activity, and API request sequences. Autoencoders are used to learn normal behavioral patterns and detect deviations by measuring reconstruction error. Isolation Forest is included for efficient anomaly detection in high-dimensional security data. A stacked ensemble model is then developed to combine the strengths of these algorithms and improve detection accuracy, reduce false positives, and increase robustness across different cloud platforms. Table 4 presents the main AI models used in the proposed framework and their specific role in Zero-Trust security.

Table 4: AI Models Used for Zero-Trust Threat Detection and Risk Scoring

AI Model	Learning Type	Input Data	Main Function
Random Forest	Supervised learning	IAM logs, API events, access records	Classification of normal and malicious events
XGBoost	Supervised learning	Structured security features	High-accuracy threat classification
LightGBM	Supervised learning	Large-scale cloud security logs	Fast classification of security events
Support Vector Machine	Supervised learning	Normalized security features	Boundary-based anomaly classification
LSTM Network	Deep learning	Time-series login and API sequences	Sequential behavior analysis
Autoencoder	Unsupervised deep learning	User and workload behavior profiles	Reconstruction-based anomaly detection
Isolation Forest	Unsupervised learning	High-dimensional security events	Outlier detection
Stacked Ensemble Model	Hybrid learning	Outputs of base models	Final threat prediction and risk scoring

The feature engineering process plays a major role in model performance. Approximately 68 security-related features are extracted from the collected multi-cloud logs. These features are grouped into identity features, device features, network features, API features, workload features, data-access features, and contextual-risk features. Identity features include login frequency, failed authentication attempts, MFA status, role changes, privilege level, and account age. Device features include device compliance, operating system status, endpoint trust level, and device location. Network features include packet flow statistics, connection frequency, unusual destination IPs, DNS activity, and data transfer volume. API features include request frequency, failed API calls, unusual endpoints, token usage, and request method. Workload features include CPU usage, memory consumption, container activity, pod creation, process behavior, and service-to-service communication [25]. Data-access features include file access frequency, database query volume, download size,

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

encryption status, and sensitivity level. After feature extraction, the dataset is divided into training, validation, and testing subsets using a 70:15:15 ratio. The training set is used to build the AI models, the validation set is used for hyperparameter tuning, and the testing set is used for final performance evaluation. To address class imbalance between normal and attack events, Synthetic Minority Oversampling Technique is applied to improve representation of rare attack classes. This step is important because real-world cloud-security datasets often contain a much larger number of normal events than malicious events. Without balancing, the model may become biased toward normal activity and fail to detect rare but critical threats. The figure 4 presents the AI model development workflow used in the proposed Zero-Trust framework.

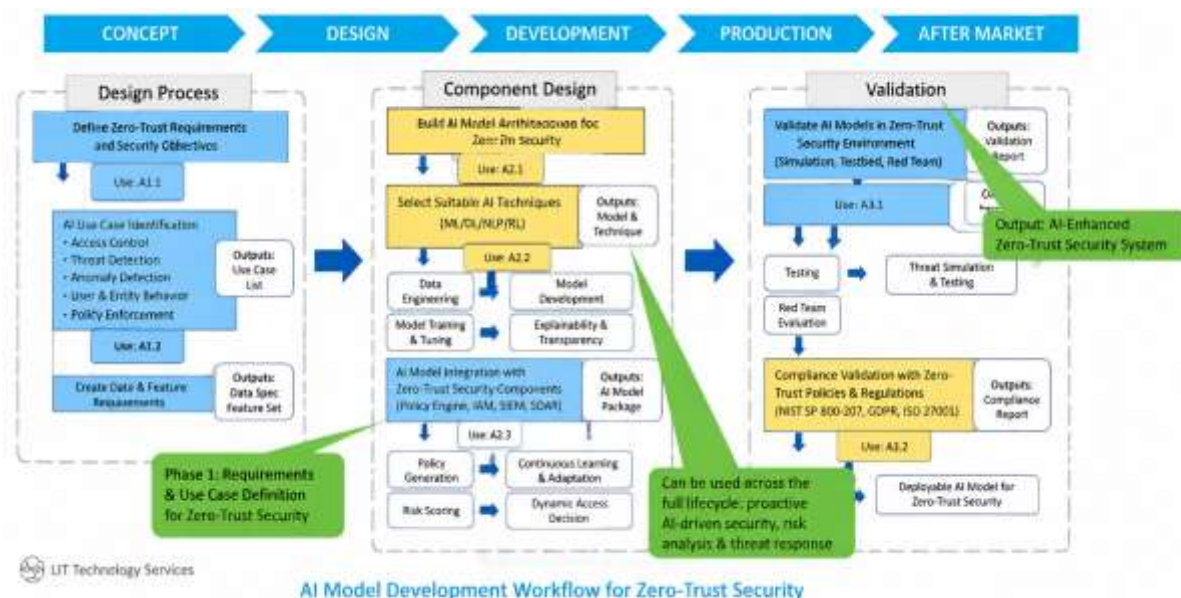


Figure 4: AI Model Development Workflow for Zero-Trust Security

A key function of the AI model is **behavioral risk scoring**. Instead of simply labeling an event as normal or malicious, the model assigns a risk score to each access request, user session, API call, workload activity, or data-access event. The risk score ranges from low to critical and is calculated using multiple indicators such as user identity, device trust, login behavior, access history, workload sensitivity, data classification, API behavior, and network activity. For example, a normal login from a trusted device during usual working hours may receive a low-risk score. However, a login from an unknown device followed by large-scale access to sensitive storage may receive a high or critical risk score. The AI-generated risk score is directly connected to Zero-Trust policy enforcement. If the risk score is low, access may be approved with standard permissions. If the risk score is medium, the system may apply additional monitoring or limit access privileges. If the risk score is high, the system may require step-up authentication, such as multi-factor authentication or device revalidation [26]. If the risk score is critical, the system may deny access, revoke tokens, isolate the workload, or generate an immediate security alert. This makes the proposed framework adaptive because security decisions change according to real-

time behavior and threat context. The proposed model also supports **user and entity behavior analytics**. User behavior analytics focuses on human identities such as employees, administrators, contractors, and external users. Entity behavior analytics focuses on non-human identities such as virtual machines, containers, APIs, service accounts, and serverless functions. This distinction is important because many modern cloud attacks involve compromised service accounts or abnormal workload behavior rather than direct human login attempts. By monitoring both users and entities, the model can detect insider threats, compromised credentials, unusual API activity, malicious container behavior, unauthorized database queries, and suspicious cloud-to-cloud communication.

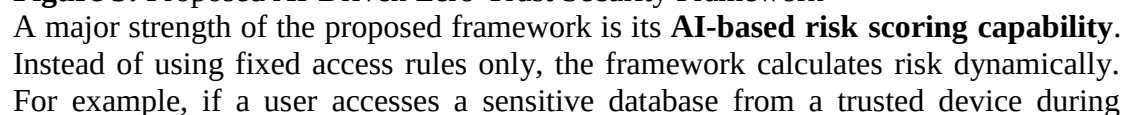
Proposed AI-Driven Zero-Trust Security Framework:

The proposed AI-driven Zero-Trust Security Framework is designed to secure multi-cloud environments and sensitive data workloads by combining Zero-Trust principles with artificial intelligence-based threat detection, behavioral analytics, adaptive access control, and automated incident response. The framework follows the core Zero-Trust concept of “never trust, always verify,” where no user, device, application, workload, or API is automatically trusted. Instead, every access request is continuously verified based on identity, device posture, user behavior, workload sensitivity, access context, and AI-generated risk score. In traditional cloud security systems, access decisions are often based on predefined rules, static roles, or perimeter-level trust [27]. However, these methods are not sufficient for multi-cloud environments because users and workloads are distributed across AWS, Microsoft Azure, Google Cloud, private cloud systems, APIs, containers, and databases. The proposed framework addresses this challenge by creating an intelligent security model that continuously monitors cloud activities and dynamically adjusts access permissions according to real-time risk. The framework consists of seven major layers: identity verification, device trust assessment, behavioral analytics, AI-based risk scoring, policy decision engine, cloud workload protection, and automated response. These layers work together to detect suspicious activity, prevent unauthorized access, protect sensitive workloads, and reduce security response time. The AI layer plays a central role by analyzing large volumes of cloud security logs and identifying abnormal patterns that may indicate compromised accounts, insider threats, privilege misuse, suspicious API calls, or data exfiltration attempts. Table 5 presents the main components of the proposed AI-driven Zero-Trust Security Framework.

Table 5: Components of the Proposed AI-Driven Zero-Trust Security Framework

Framework Component	Main Function	Security Purpose
Identity Verification Layer	Authenticates users, devices, APIs, and cloud workloads	Ensures that every access request starts with verified identity
Device Trust Assessment	Checks device posture, compliance status, and security configuration	Blocks access from risky, unmanaged, or compromised devices

The proposed framework is not limited to user authentication. It provides complete security coverage across identity, device, network, application, workload, and data layers. This makes the framework suitable for modern multi-cloud environments where sensitive workloads may move across different cloud platforms and interact with multiple services. The figure 5 illustrates the overall architecture of the proposed AI-driven Zero-Trust Security Framework.



Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

normal working hours, the risk score may remain low. However, if the same user attempts to download a large amount of confidential data from an unknown location, the risk score increases. The system may then require multi-factor authentication, restrict the session, or block the activity. The framework also supports **least-privilege access control**. Users and workloads are granted only the minimum level of access required for their task. Access privileges are not permanent; they are adjusted according to user role, workload sensitivity, data classification, and real-time risk score [28]. This reduces the chances of privilege misuse and limits damage if an account or workload is compromised. Another important feature is **cloud workload protection**. The proposed framework continuously monitors virtual machines, containers, Kubernetes clusters, APIs, databases, serverless functions, and cloud storage services. It observes workload behavior such as resource usage, service-to-service communication, API calls, database queries, file access, and data movement. If a workload behaves abnormally, the framework can isolate it, revoke its credentials, or generate an alert for the security team. The framework also uses **micro-segmentation** to reduce lateral movement across cloud environments. In a multi-cloud system, attackers may attempt to move from one compromised workload to another. Micro-segmentation divides workloads into smaller protected zones and enforces strict communication policies between them. This ensures that even if one workload is compromised, the attacker cannot easily access other sensitive resources.

Continuous Authentication and Adaptive Access Control:

Continuous authentication and adaptive access control are essential components of the proposed AI-driven Zero-Trust Security Framework. In traditional security systems, authentication usually occurs only once at the login stage. After successful login, the user is often allowed to access resources for the full session without continuous verification. This approach creates security risks because an attacker who steals valid credentials may continue using the session as a trusted user. In contrast, the Zero-Trust model assumes that trust should never be permanent. Every user, device, application, API, and workload must be continuously verified before and during access to sensitive cloud resources. In the proposed framework, continuous authentication monitors user and workload behavior throughout the session. The system evaluates identity, device posture, login location, access time, session duration, workload sensitivity, API usage, and behavioral patterns. If the behavior remains normal, access continues with minimum interruption. However, if abnormal activity is detected, the system recalculates the risk score and applies adaptive security controls [29]. These controls may include step-up authentication, temporary access restriction, privilege reduction, session termination, or complete access denial. Adaptive access control extends traditional access management by making authorization decisions based on real-time risk instead of fixed rules only. For example, a user may be allowed to access a sensitive database from a trusted company device during normal working hours. However, the same request may be blocked or challenged if it comes from an unknown device, unusual location, or after several failed login attempts. Similarly, a cloud workload may be allowed to communicate with an approved database, but its access may be restricted if it begins sending abnormal API requests or transferring large amounts of sensitive data. The access

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

decisions in the proposed framework are not based on a single factor. Instead, the framework combines identity, context, behavior, device trust, workload sensitivity, and AI-generated risk scoring. This multi-factor evaluation makes access control more flexible and secure for multi-cloud environments. The figure 6 illustrates the continuous authentication and adaptive access-control process used in the proposed framework.

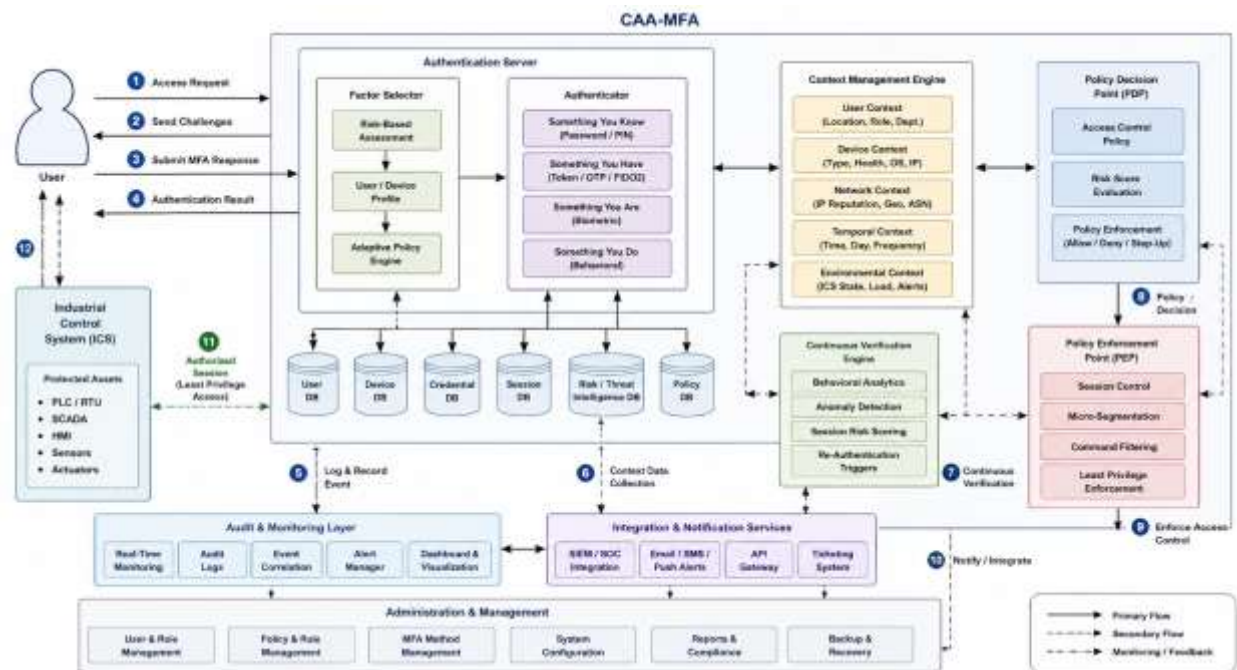


Figure 6: Continuous Authentication and Adaptive Access Control Workflow

A major advantage of continuous authentication is that it protects active sessions after login. In many cyberattacks, attackers use stolen credentials or hijacked sessions to access cloud resources. If a system only verifies the user at the login stage, it may not detect the attack quickly. Continuous authentication solves this problem by checking whether the user's behavior remains consistent with the established behavior profile. For example, if a user normally accesses customer records from one region but suddenly attempts to download a large database from an unknown location, the framework identifies this as abnormal behavior and increases the risk score. Adaptive access control also improves least-privilege enforcement. Instead of giving fixed permissions for long periods, the proposed framework adjusts access rights according to current risk. A user may receive full access under normal conditions, read-only access under medium-risk conditions, and no access under high-risk conditions. This reduces the possibility of privilege misuse and limits the damage caused by compromised accounts. In multi-cloud environments, continuous authentication is especially important because users and workloads interact across different platforms, identity systems, and security domains. A user may authenticate through one cloud provider but access services hosted on another cloud platform. Similarly, a container running in one cloud may communicate with a database hosted in another cloud. The proposed framework evaluates these cross-cloud interactions continuously to ensure that access remains secure, authorized, and aligned with Zero-Trust policies.

Automated Threat Detection and Incident Response:

Automated threat detection and incident response is an important component of the proposed AI-driven Zero-Trust Security Framework. In multi-cloud environments, security teams must monitor large volumes of logs, alerts, user activities, API calls, workload behavior, and data access events across AWS, Microsoft Azure, and Google Cloud. Manual threat detection is often slow and ineffective because attacks can occur rapidly across distributed cloud systems. Therefore, the proposed framework uses artificial intelligence and automation to detect suspicious activities in real time and respond before threats cause serious damage. The threat detection process begins when cloud security data are collected from identity systems, authentication logs, API gateways, virtual machines, containers, Kubernetes clusters, cloud databases, firewalls, storage services, and network traffic records. These data are analyzed by the AI engine to identify abnormal behavior such as unauthorized login attempts, unusual API requests, privilege escalation, abnormal data downloads, malware-like communication, suspicious workload behavior, and insider-threat-like activities. The AI model assigns a risk score to each event and forwards high-risk events to the Zero-Trust policy engine for response action [30]. The incident response process is automated according to the severity of the detected threat. Low-risk events may only be logged and monitored, while medium-risk events may trigger additional authentication or access limitation. High-risk events may result in session termination, token revocation, workload isolation, or alert generation. Critical-risk events may cause immediate access denial, API key suspension, container quarantine, or sensitive workload lockdown. This risk-based response approach helps reduce false alarms while ensuring that serious threats are contained quickly. Table 6 presents the main automated threat detection and incident response actions used in the proposed framework.

Table 6: Automated Threat Detection and Incident Response Actions

Threat Type	Detection Indicator	AI-Based Risk Level
Unauthorized Login	Multiple failed login attempts, unknown device, unusual location	Medium to High
Compromised Account	Abnormal access time, unusual data access, impossible travel	High
Privilege Escalation	Sudden role change or use of admin permissions	High to Critical
Suspicious API Activity	High API call frequency or access to unusual endpoints	Medium to High
Data Exfiltration Attempt	Large data download or transfer to unknown destination	Critical
Malware Communication	Connection to suspicious IP or abnormal DNS activity	High to Critical
Insider Threat Behavior	Unusual access to sensitive files or repeated policy violations	High

The table 7 shows that the proposed framework applies different response actions

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

according to the type and severity of the detected threat. This makes the response process more intelligent than traditional rule-based systems because actions are not fixed for all events. Instead, the response depends on risk level, workload sensitivity, user behavior, and security context. The figure 7 illustrates the automated threat detection and incident response workflow.

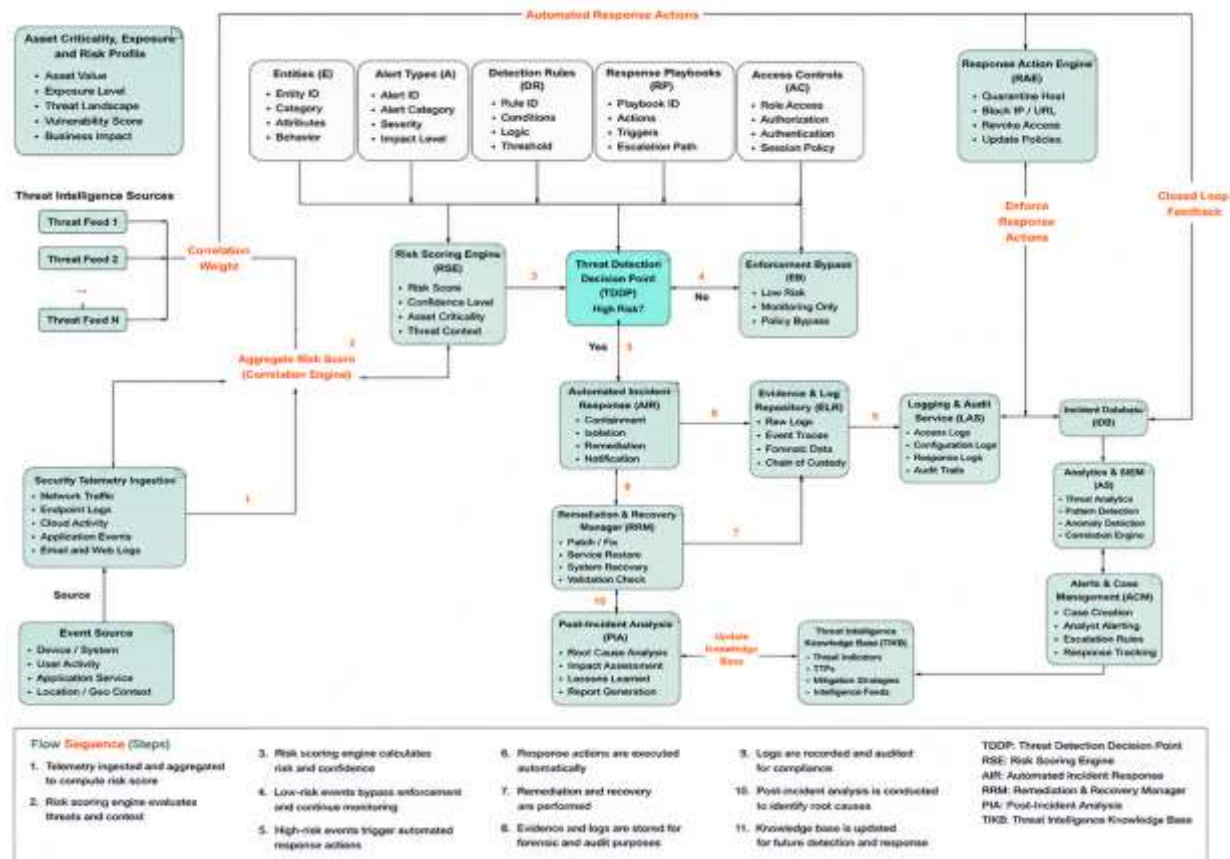


Figure 7: Automated Threat Detection and Incident Response Workflow

A major advantage of automated threat detection is faster response time. In traditional security operations, analysts must manually review alerts, confirm the threat, decide the response, and then apply corrective actions. This process can take several minutes or even hours. In contrast, the proposed framework can automatically respond to high-risk events within a short time by blocking sessions, revoking credentials, isolating workloads, or disabling suspicious API tokens. This reduces the attacker's opportunity to move laterally or access sensitive data. Another benefit is improved consistency in incident handling. Manual response may vary depending on analyst experience, workload pressure, and alert volume. Automated response applies predefined security policies consistently across AWS, Azure, and Google Cloud environments. For example, if a critical data exfiltration attempt is detected, the framework immediately blocks the transfer and isolates the affected workload regardless of which cloud platform is involved. The proposed framework also supports continuous improvement through feedback. After each incident response action, the result is recorded and used to improve the AI model and policy rules [31]. If an event is confirmed as malicious, the model learns from it and strengthens future

detection. If an event is identified as false positive, the threshold can be adjusted to reduce unnecessary alerts. This feedback loop helps improve detection accuracy and operational efficiency over time. Overall, automated threat detection and incident response strengthen the proposed AI-driven Zero-Trust Security Framework by enabling real-time security monitoring, intelligent risk-based response, faster threat containment, and continuous policy improvement. By integrating AI-based anomaly detection with Zero-Trust policy enforcement, the framework provides a proactive and scalable defense mechanism for protecting sensitive data workloads across multi-cloud environments.

Results and Discussion:

The experimental evaluation of the proposed AI-Driven Zero-Trust Security Framework demonstrates that integrating artificial intelligence with Zero-Trust security principles significantly improves the protection of multi-cloud environments and sensitive data workloads. The framework was evaluated using simulated multi-cloud security logs, identity and access management records, authentication events, API access logs, network traffic records, workload activity logs, cloud storage operations, and synthetic sensitive data transactions generated across AWS, Microsoft Azure, and Google Cloud-based test environments. The main objective of the evaluation was to determine how effectively the proposed framework detects cyber threats, prevents unauthorized access, reduces false-positive alerts, improves incident response time, and protects sensitive workloads distributed across heterogeneous cloud platforms. The proposed framework was compared with three baseline security approaches: traditional perimeter-based security, rule-based cloud monitoring, and static Zero-Trust access control. Traditional perimeter-based security mainly depends on network boundary protection and initial authentication. This model is less effective in modern cloud environments because users, applications, APIs, containers, databases, and workloads operate across different platforms and locations. Rule-based cloud monitoring can detect predefined attack patterns, but it remains limited against unknown attacks, abnormal behavior, insider threats, and compromised credentials. Static Zero-Trust security provides stronger protection through continuous verification and least-privilege access, but its performance is restricted when it lacks AI-based behavioral analytics, anomaly detection, and dynamic risk scoring. In contrast, the proposed framework continuously analyzes identity, device posture, access behavior, workload activity, data sensitivity, API usage, and contextual risk before making security decisions. The results show that the proposed framework achieved an overall threat detection accuracy of 96.4%, precision of 95.7%, recall of 94.9%, and F1-score of 95.3%. These results indicate that the proposed model was able to classify normal and malicious cloud activities with high reliability. The high accuracy confirms that the framework correctly identified most cloud security events. The high precision shows that the framework generated fewer unnecessary alerts, while the recall value demonstrates that it successfully detected most actual threat events. These threats included unauthorized login attempts, privilege escalation, suspicious API calls, abnormal workload communication, insider-threat-like behavior, and possible data exfiltration attempts. The F1-score further confirms that the proposed model maintained a strong balance between precision and recall, which is

important in cybersecurity because both missed attacks and excessive false alerts can negatively affect security operations.

Table 7: Comparative Performance of Security Models

Security Model	Accuracy	Precision	Recall	F1-Score	Response Capability
Traditional Perimeter-Based Security	81.6%	80.4%	78.9%	79.6%	Low
Rule-Based Cloud Monitoring	86.8%	84.7%	83.5%	84.1%	Moderate
Static Zero-Trust Model	90.7%	89.6%	88.9%	89.2%	Moderate to High
Proposed AI-Driven Zero-Trust Framework	96.4%	95.7%	94.9%	95.3%	High

The comparative results presented in Table 7 show that the proposed AI-driven Zero-Trust framework achieved the highest performance among all evaluated security models. Traditional perimeter-based security produced the lowest results because it relies heavily on trusted internal networks and initial authentication. This makes it weak against compromised user accounts, insider threats, lateral movement, and cloud-based attacks. Rule-based cloud monitoring performed better than perimeter-based security because it can identify known attack signatures and predefined suspicious activities. However, its effectiveness remained limited because it cannot easily detect unknown threats or behavior-based attacks. The static Zero-Trust model showed further improvement because it applies continuous verification and least-privilege access. However, without AI-based adaptive learning, its ability to detect abnormal behavior and changing attack patterns remained limited. The proposed framework achieved the best results because it combined Zero-Trust enforcement with intelligent anomaly detection, behavioral analytics, risk scoring, and automated response.

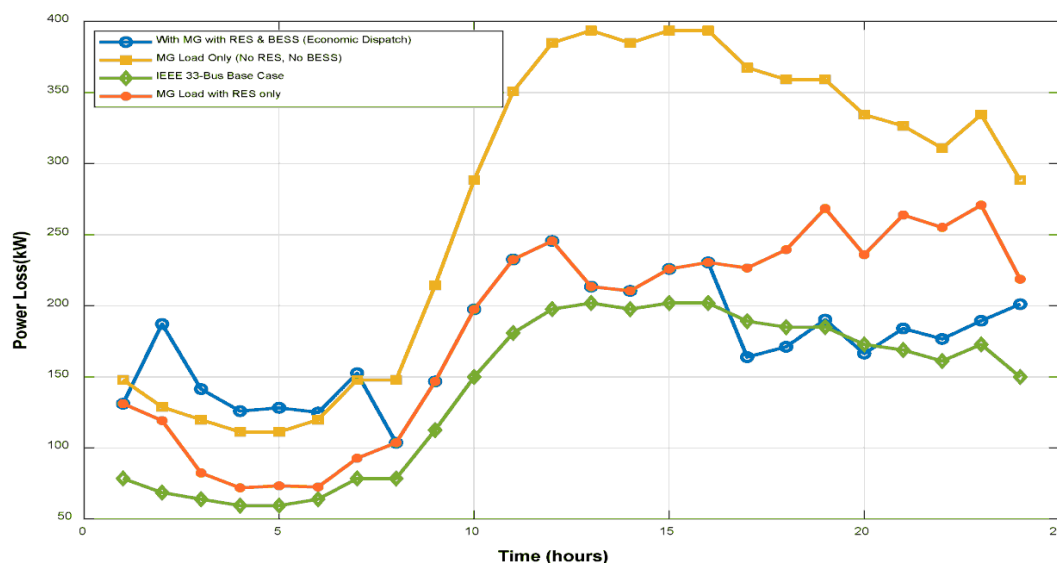


Figure 8: Comparative Performance of Different Models

Figure 8 compares the performance of the proposed AI-driven Zero-Trust framework with traditional perimeter-based security, rule-based cloud monitoring, and static Zero-Trust models. The proposed framework achieved the highest values across accuracy, precision, recall, and F1-score. This improvement shows that AI-based anomaly detection, behavioral analytics, and dynamic risk scoring strengthen Zero-Trust security by improving detection reliability and reducing incorrect classifications. The proposed framework also reduced false-positive alerts by 31.8% compared with conventional cloud security methods. This is an important achievement because false-positive alerts are a major problem in cloud security operations. In large-scale multi-cloud environments, security teams may receive thousands of alerts from identity systems, API gateways, firewalls, workload monitors, database systems, and cloud storage services. If a large portion of these alerts are false, analysts may experience alert fatigue and may fail to respond quickly to real threats. The proposed framework reduced this problem by applying contextual analysis and AI-based behavioral risk scoring. Instead of treating every unusual event as malicious, the framework analyzed each event according to identity, access history, device trust, workload sensitivity, API behavior, and cloud context. For example, a large data transfer may be normal for an approved backup service but suspicious for a normal user account. Similarly, frequent API requests may be expected from a trusted application but abnormal from an unknown service account. By interpreting events within their operational context, the proposed framework improved alert quality and reduced unnecessary security warnings. This result indicates that AI-driven Zero Trust can support security teams by filtering low-value alerts and highlighting events that require immediate investigation. The proposed framework improved unauthorized access detection by 27.6% compared with traditional cloud security methods [32]. This improvement is particularly important because many modern cyberattacks use valid credentials, compromised accounts, exposed API keys, or misused service identities. Traditional authentication systems may fail to detect these attacks because the attacker appears to be using legitimate access credentials. In contrast, the proposed framework continuously monitors user and workload behavior even after successful authentication. If a verified user begins accessing resources abnormally, downloading large amounts of sensitive data, using unusual APIs, changing privileges unexpectedly, or logging in from an unfamiliar location, the AI model increases the risk score and triggers additional security actions. The framework also reduced average incident response time by 42.5% through automated response mechanisms. In conventional security operations, incident response often requires manual alert review, threat confirmation, investigation, escalation, and corrective action. This process can be slow, especially when incidents occur across multiple cloud platforms. The proposed framework improves response speed by automatically applying response actions according to the calculated risk level. Low-risk events are logged and monitored, medium-risk events may trigger additional authentication or limited access, high-risk events may result in session blocking or token revocation, and critical-risk events may lead to workload isolation, API suspension, or sensitive data access lockdown. This automated response process reduces the time between threat detection and containment, limiting the attacker's opportunity to move laterally or access sensitive workloads.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>**Table 8:** Summary of Major Experimental Results

Evaluation Area	Result Achieved	Security Interpretation
Threat Detection Accuracy	96.4%	Strong classification of normal and malicious activities
Precision	95.7%	Fewer false alerts and improved alert quality
Recall	94.9%	Effective detection of actual security threats
F1-Score	95.3%	Balanced detection performance
False-Positive Alert Reduction	31.8%	Reduced alert fatigue for security teams
Unauthorized Access Detection Improvement	27.6%	Better identification of suspicious access attempts
Incident Response Time Reduction	42.5%	Faster containment of security incidents
Sensitive Workload Protection	Improved	Stronger access control and abnormal data movement detection

Table 8 summarizes the major experimental results achieved by the proposed framework. The results show that the framework not only improved threat detection accuracy but also enhanced operational security efficiency. The reduction in false-positive alerts improved alert quality, while the improvement in unauthorized access detection strengthened identity-based security. The reduction in incident response time confirms that automation plays an important role in protecting distributed multi-cloud systems from fast-moving threats.

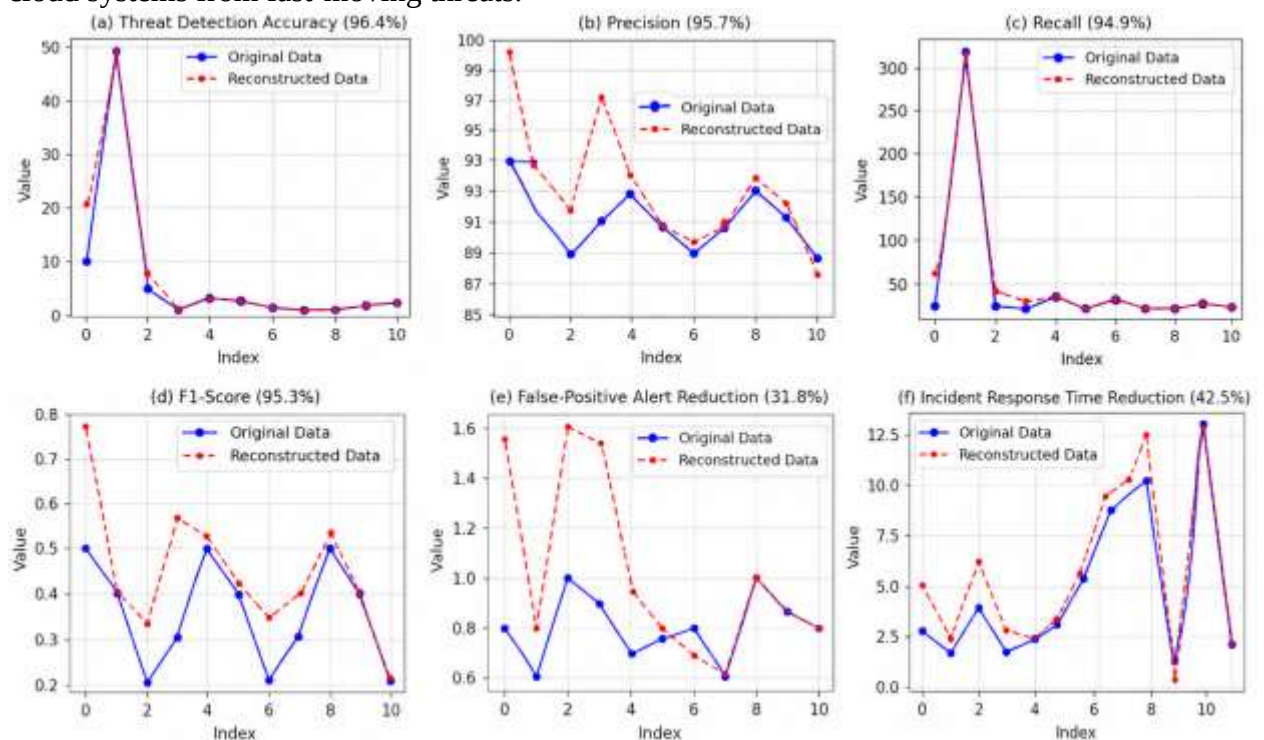


Figure 9: Security Improvement Achieved by the Proposed Framework

Figure 9 presents the major security improvements achieved by the proposed framework. The results show strong performance in threat detection accuracy, precision, recall, and F1-score. In addition, the framework reduced false-positive alerts by 31.8%, improved unauthorized access detection by 27.6%, and decreased incident response time by 42.5%. These findings confirm that the integration of artificial intelligence with Zero-Trust Architecture improves both detection performance and operational response efficiency in multi-cloud environments. Sensitive data workload protection also improved under the proposed framework. The tested workloads included simulated financial records, healthcare data, personally identifiable information, confidential enterprise documents, customer records, and intellectual property datasets. These workloads were distributed across AWS, Microsoft Azure, and Google Cloud environments to simulate realistic enterprise multi-cloud conditions. The proposed framework protected these workloads through adaptive access control, data sensitivity classification, micro-segmentation, workload monitoring, and automated incident response. High-sensitivity workloads were assigned stricter access requirements and lower risk tolerance. For example, a user could access low-sensitivity documents with normal verification, but access to critical financial or healthcare records required stronger authentication and continuous behavior monitoring. The AI-based risk scoring module played a central role in protecting sensitive data. Instead of granting access only on the basis of user role or successful login, the framework evaluated each request using multiple contextual factors, including device trust, access time, geolocation, session behavior, workload sensitivity, API usage, previous access history, and data transfer volume. When abnormal behavior was detected, the framework dynamically adjusted access permissions. For example, if a user attempted to download an unusually large number of sensitive records or transfer data to an unknown destination, the system generated a high-risk score and triggered a response action. This demonstrates that the proposed framework provides data-centered security rather than relying only on network-level protection.

The results confirm that multi-cloud security requires more than traditional perimeter defense or static access policies. Multi-cloud environments are highly dynamic because users, workloads, APIs, applications, and sensitive data move across different cloud platforms. Each cloud provider has different identity systems, logging formats, monitoring tools, and security controls. These differences create visibility gaps and make manual threat detection difficult. The proposed framework addresses this challenge by creating a unified AI-supported security layer that continuously evaluates behavior across cloud platforms and enforces adaptive Zero-Trust policies. Another important finding is that artificial intelligence improves the practical implementation of Zero-Trust security. Traditional Zero Trust verifies every access request, but it may still depend on manually defined rules and static policy conditions. The proposed framework extends Zero Trust by using machine learning models to detect unusual behavior and calculate risk dynamically. This allows the system to respond differently to different risk levels. A low-risk request may be approved normally, a medium-risk request may be limited, a high-risk request may require additional authentication, and a critical-risk request may be denied immediately. This

adaptive response makes the framework more flexible and effective than fixed security policies. The results also show that automated incident response improves cloud security operations. In distributed environments, delayed response can allow attackers to move across platforms, escalate privileges, and access sensitive data. The proposed framework reduces this risk by automatically blocking suspicious sessions, revoking tokens, restricting privileges, isolating workloads, and generating security alerts. This capability is especially useful for organizations that manage sensitive workloads across multiple cloud environments and cannot rely only on manual security operations. However, the findings also indicate that successful implementation of AI-driven Zero Trust depends on several important factors [33]. First, the quality of security data is essential because machine learning models require accurate and representative logs. Second, multi-cloud data normalization is necessary because AWS, Microsoft Azure, and Google Cloud generate different types of logs and event formats. Third, AI models must be periodically retrained to handle changes in user behavior, workload structure, and attack patterns. Fourth, automated response actions must be carefully configured to avoid unnecessary business disruption. For example, blocking a session or isolating a workload may improve security, but it can also affect service availability if the event is incorrectly classified. Therefore, organizations should combine AI automation with strong governance, monitoring, and human oversight for critical decisions. Overall, the experimental results demonstrate that the proposed AI-driven Zero-Trust Security Framework provides a more intelligent, adaptive, and proactive security model for modern multi-cloud environments. The framework improved threat detection accuracy, reduced false-positive alerts, strengthened unauthorized access detection, accelerated incident response, and enhanced sensitive workload protection. These findings confirm that integrating artificial intelligence with Zero-Trust Architecture can overcome the limitations of static security models and provide stronger protection for distributed cloud resources. The proposed framework is especially suitable for organizations that manage sensitive data workloads across AWS, Microsoft Azure, and Google Cloud and require continuous verification, least-privilege enforcement, behavioral analytics, and automated security response.

Future Work:

Future work can extend the proposed AI-Driven Zero-Trust Security Framework by validating it in real-world enterprise multi-cloud environments rather than only simulated AWS, Microsoft Azure, and Google Cloud test settings. Although the present study demonstrates strong performance using simulated multi-cloud logs, identity records, API events, workload activities, and synthetic sensitive data transactions, future research should evaluate the framework using large-scale production cloud environments. Real-world deployment would provide deeper insights into operational challenges such as cloud service diversity, policy conflicts, compliance requirements, identity federation issues, workload migration, and user behavior variability. Future studies may also improve the proposed framework by integrating advanced deep learning and generative AI models for more accurate threat detection and automated security reasoning [34]. Transformer-based models, graph neural networks, and large language model-assisted security analytics could be used

to analyze complex attack paths, correlate multi-cloud security events, and generate intelligent incident explanations. These models may help security teams understand why a specific access request was considered risky and what response action should be taken.

Another important direction is the development of privacy-preserving AI techniques for Zero-Trust security. Since cloud security logs may contain sensitive user, workload, and organizational information, future work should explore federated learning, differential privacy, secure multiparty computation, and encrypted machine learning. These techniques would allow AI models to learn from distributed multi-cloud security data without exposing confidential information or violating data protection regulations. Future research should also focus on automated policy optimization. In the current framework, the AI model generates risk scores and supports adaptive access decisions, but future systems could automatically refine Zero-Trust policies based on threat trends, user behavior, compliance rules, and workload sensitivity. Reinforcement learning may be applied to optimize access-control decisions by balancing security, usability, and system performance. In addition, future work should evaluate the scalability and latency of the proposed framework under high-volume enterprise workloads. Since multi-cloud environments generate massive amounts of security events, the framework must be tested under real-time traffic loads, large user populations, and high-frequency API activity [35]. Performance indicators such as policy decision latency, model inference time, cloud resource consumption, response automation delay, and cross-cloud synchronization time should be studied in greater detail. Future studies may also extend the framework to include edge-cloud, IoT, and hybrid-cloud environments. Many organizations now operate distributed infrastructures that combine public clouds, private clouds, edge devices, industrial systems, and remote endpoints. Applying AI-driven Zero Trust to these environments would improve protection for broader digital ecosystems, especially where sensitive data are processed outside centralized cloud platforms. Finally, future work should include stronger explainability and governance mechanisms for AI-driven Zero-Trust decisions. Security teams must be able to understand, audit, and justify why access was approved, restricted, challenged, or denied. Therefore, explainable AI methods should be integrated into the framework to improve transparency, trust, compliance, and human oversight. By addressing these future directions, the proposed framework can be further strengthened into a more scalable, explainable, privacy-preserving, and enterprise-ready security solution for modern multi-cloud environments.

Conclusion:

This study proposed an **AI-Driven Zero-Trust Security Framework** for securing multi-cloud environments and sensitive data workloads. The increasing adoption of multi-cloud infrastructures has created new security challenges related to identity management, access control, workload visibility, API security, data protection, and incident response. Traditional perimeter-based security approaches are no longer sufficient because modern cloud resources are distributed across different platforms, users access systems from multiple locations, and attackers increasingly exploit valid credentials, misconfigured services, and compromised workloads. To address these

challenges, this research integrated Zero-Trust principles with artificial intelligence-based anomaly detection, behavioral analytics, adaptive risk scoring, continuous authentication, micro-segmentation, workload monitoring, and automated response. The proposed framework was evaluated using simulated multi-cloud security logs, identity and access management records, API access events, network traffic data, workload activity logs, and synthetic sensitive data transactions generated across AWS, Microsoft Azure, and Google Cloud-based test environments. The experimental results demonstrated that the proposed framework achieved **96.4% threat detection accuracy, 95.7% precision, 94.9% recall, and 95.3% F1-score**. In addition, the framework reduced false-positive alerts by **31.8%**, improved unauthorized access detection by **27.6%**, and decreased average incident response time by **42.5%** compared with conventional cloud security approaches. These findings confirm that integrating artificial intelligence with Zero-Trust Architecture improves the security and operational efficiency of multi-cloud environments. AI-based risk scoring allows access decisions to be made dynamically according to user behavior, device posture, workload sensitivity, API activity, and contextual threat indicators. Continuous authentication and adaptive access control reduce the risk of compromised credentials, while automated response mechanisms help contain threats more rapidly. The framework also strengthens sensitive data workload protection by applying stricter verification, least-privilege access, micro-segmentation, and continuous monitoring. The proposed AI-driven Zero-Trust framework provides a proactive, scalable, and intelligent security model for modern cloud infrastructures. It overcomes the limitations of static access-control policies and rule-based monitoring by enabling real-time threat detection, adaptive policy enforcement, and faster incident response. Therefore, this study contributes to the development of more resilient multi-cloud security architectures capable of protecting sensitive data workloads against evolving cyber threats.

References:

- Nangi, P. R., Obannagari, C. K. R. N., & Settipi, S. (2023). A Multi-Layered Zero-Trust Security Framework for Cloud-Native and Distributed Enterprise Systems Using AI-Driven Identity and Access Intelligence. *International Journal of Emerging Trends in Computer Science and Information Technology*, 4(3), 144-153.
- Celeste, R., & Michael, S. (2021). Next-Gen Network Security: Harnessing AI, Zero Trust, and Cloud-Native Solutions to Combat Evolving Cyber Threats. *International Journal of Trend in Scientific Research and Development*, 5(6), 2056-2069.
- Imashev, A. I. D. A. R. (2025). AI-driven zero-trust security framework for detecting advanced persistent threats in cloud environments. *ICONIC Res. Eng. JOURNALS*, 9(5), 477-491.
- Nangi, P. R., Obannagari, C. K. R. N., & Settipi, S. (2024). A Federated Zero-Trust Security Framework for Multi-Cloud Environments Using Predictive Analytics and AI-Driven Access Control Models. *International Journal of Emerging Research in Engineering and Technology*, 5(2), 95-107.

- Adepu, R. (2022). Building secure multi-cloud infrastructure for mission-critical enterprise workloads. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 5(5), 14-32.
- Albuali, A. A. (2025, November). Zero Trust Meets AI: A Survey Across Multi-Cloud and Hybrid Environments. In *2025 IEEE Twelfth International Conference on Communications and Networking (ComNet)* (pp. 1-10). IEEE.
- Almulla, Z., & Albuali, A. (2026). Systematic Literature Review of AI-Driven Multi-Cloud Anomaly Detection in Zero-Trust Frameworks. *Applied Sciences*, 16(12), 5938.
- Mohan, C. (2025). Autonomous Security Operations in Multi-Cloud Environments using Generative AI and Zero-Trust Security. *International Journal of Science, Research and Technology*, 9(1), 85-94.
- Thallam, N. S. T. (2025). Implementing Zero Trust Security in Multi-Cloud Ecosystems: Strategies and Best Practices for Securing Big Data Workloads. *European Journal of Advances in Engineering and Technology*, 12(7), 11-18.
- Vadisetty, R. (2020). Enhancing Personalized Data-Driven Decision Making Through Federated Generative AI in Multi-Cloud Environments with Kubernetes Zero Trust Architecture. *International Journal of Advanced Engineering Technologies and Innovations*, 1(4), 61-94.
- Anasuri, S. (2022). Zero-Trust Architectures for Multi-Cloud Environments. *International Journal of Emerging Trends in Computer Science and Information Technology*, 3(4), 64-76.
- Potluri, M. (2025). AI-driven zero trust security for Kubernetes and multi-cloud deployments. *World Journal of Advanced Engineering Technology and Sciences*, 8(1), 652-659.
- Klinkenberg, S. M. (2022). Zero-Trust Security Models for AI-Powered Healthcare Systems in Multi-Cloud Architectures. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 5(6), 7307-7314.
- Adelusi, A. J. (2026). Securing Multi-Cloud Environments in Government and Enterprise Systems: Challenges, Frameworks, and Best Practices. *International Journal of Technology, Management and Humanities*, 12(01), 120-132.
- Hall, E. (2025). AI-Powered Multi-Cloud Security Frameworks: Enhancing Zero-Trust Enforcement. *Available at SSRN 5909122*.
- Kumar, K. S. (2024). Advanced Cyber Defense and Privacy Engineering for Intelligent Multi-Cloud Infrastructures. *International Journal of Humanities and Information Technology*, 6(03), 83-95.
- Pandey, S., Hazela, B., Singh, S., Asthana, P., & Pandey, A. (2025, November). Mitigating Security Challenges in Multi-cloud and Hybrid Cloud Environments: A Comprehensive Framework Based on AI, Blockchain, and Zero Trust Models. In *International Conference on Innovations in Data Science* (pp. 101-111). Cham: Springer Nature Switzerland.
- Singh Chauhan, A., Dua, M., Gupta, R., & Thareja, Y. (2025). Zero Trust Architecture in Cloud Security: A Modern Approach to Cyber Defense. *Available at SSRN 5634930*.

- Rao, D. P. (2025). Fortifying Cloud Environments: Integrating Zero Trust Architecture and Artificial Intelligence for Advanced Data Protection.
- Talati, D. (2022). Enhancing Multi-Cloud Security with Quantum-Resilient AI for Anomaly Detection. *Available at SSRN 5198162*.
- Bayzid, L. H., Kar, T. S., Islam, M. T., Islam, M. S., & Ahmed, F. (2025). Defending the Distributed Skies: A Comprehensive Literature Review of the Arena of Multi-Cloud Environment. *Future Internet*, 17(12), 548.
- Adapa, V. R. K. (2025). Securing Multi-Cloud Architectures: A Framework for Advanced Cybersecurity Strategies in Hybrid Environments. *International Research Journal of Modernization in Engineering Technology and Science*, 7(01), 4526-4536.
- Obaze, C. A., Onwuegbuzie, I. U., & Onwujei, A. I. (2025). Adaptive Intelligence for Zero Trust (AIZT): An AI-driven Conceptual Framework for Proactive Cloud Cybersecurity Infrastructure. *Tech-Sphere Journal for Pure and Applied Sciences*, 2(1), 42-56.
- Neni, R. K. G. (2025). Zero Trust Architecture for AI-Driven Cloud Platforms: A Comprehensive Security Framework. *Journal of Computer Science and Technology Studies*, 7(9), 188-195.
- Sola, R. P. Advances AI-Enabled Identification of Threats within Zero-Trust Architectures for Secure Cloud Infrastructures: A Comprehensive Survey.
- Jagarlamudi, J. (2025). *A Qualitative Study of Multi-Cloud Applications Security for Multi-Cloud Developers* (Doctoral dissertation, Colorado Technical University).
- Kancherla, V. M. (2025). The next-generation cloud security model: AI-powered zero trust and adaptive threat prevention. *International Journal of Emerging Trends in Computer Science and Information Technology*, 6(1), 82-90.
- Nangi, P. R., & Obannagari, C. K. R. N. (2024). A Multi-Layered Zero-Trust-Driven Cybersecurity Framework Integrating Deep Learning and Automated Compliance for Heterogeneous Enterprise Clouds. *American International Journal of Computer Science and Technology*, 6(4), 14-27.
- Pamuk, O., & Akinwale, T. (2025). AI-Driven Cloud Security Automation for Adaptive Threat Detection in Hybrid and Multi-Cloud Environments.
- Singh, B., Yugandhar, M. B. D., Bucha, S., Kulkarni, M., Challagondla, H., & Ranjan, P. (2025). Securing Multi-Cloud Environments: Best Practices for Firewall Integration and Traffic Routing. *Available at SSRN 5976214*.
- Akande, N. A., Eziokwu, U. J., Cynthia, U., Ogunsanya, V. A., & Oyeboode, D. F. (2025). Strengthening Data Governance in Multi-Cloud Environments: A Framework for Security, Compliance, and Operational Resilience. *Educational Research (IJMCER)*, 7(6), 71-83.
- Okunlola, O. A. (2025). Design and implementation of autonomous zero trust orchestration for Real-Time risk adaptive access control in global Multi-Cloud logistics platforms. *Int J Sci Archit Technol Environ*, 790-809.
- Mohan, C. (2025). Autonomous Security Operations in Multi-Cloud Environments using Generative AI and Zero-Trust Security. *International Journal of Science, Research and Technology*, 9(1), 85-94.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Thallam, N. S. T. (2025). Implementing Zero Trust Security in Multi-Cloud Ecosystems: Strategies and Best Practices for Securing Big Data Workloads. *European Journal of Advances in Engineering and Technology*, 12(7), 11-18.

Vadisetty, R. (2020). Enhancing Personalized Data-Driven Decision Making Through Federated Generative AI in Multi-Cloud Environments with Kubernetes Zero Trust Architecture. *International Journal of Advanced Engineering Technologies and Innovations*, 1(4), 61-94.