Threat Assessment Report

Project: AI application_v1

Date: January 31, 2026

COMPREHENSIVE THREAT ASSESSMENT REPORT

AI Application - Cloud Web Application (AWS)

EXECUTIVE SUMMARY

Overall Risk Rating: CRITICAL

This assessment analyzed the uploaded architecture documentation (samplearchitecture.png) for the AI application deployed on AWS cloud infrastructure. The review identified multiple critical security gaps across all risk categories, with particular concerns around exposed services, lack of network segmentation, and insufficient security controls for an AI-enabled web application handling potentially sensitive data.

Top 5 Critical Findings (with Document Evidence & Examples)

Finding	Evidence Source (Doc)	Example from Docs	Risk Level	Business Impact	Timeline
F001 - Public Internet Exposure	Document: samplearchitecture.png	Direct internet access to web application without apparent security gateway	CRITICAL	Complete system compromise, data breach	Immediate (0-30 days)
F002 - Insufficient Network Segmentation	Document: samplearchitecture.png	Database and application components appear in same network tier	CRITICAL	Lateral movement, data exfiltration	Immediate (0-30 days)
F003 - Missing Security Controls Visibility	Document: samplearchitecture.png	No visible WAF, security monitoring, or access controls	HIGH	Undetected attacks, compliance violations	Short-term (30-90 days)
F004 - AI Model Protection Gaps	Document: samplearchitecture.png	AI components directly accessible without isolation	HIGH	Model theft, adversarial attacks	Short-term (30-90 days)
F005 - Single Points of Failure	Document: samplearchitecture.png	Limited redundancy visible in architecture	HIGH	Service disruption, availability impact	Short-term (30-90 days)

Key Recommendations Summary

Priority	Count	Sample Actions
P0 - **CRITICAL**	3	Implement WAF, network segmentation, access controls
P1 - **HIGH**	5	Add monitoring, encrypt data flows, secure AI models
P2 - **MEDIUM**	4	Enhance logging, implement backup strategies, compliance controls

---

THREAT MODELING ANALYSIS - MITRE ATT&CK;

Summary: Analysis of the architecture diagram reveals multiple attack vectors across the MITRE ATT&CK framework, with particular vulnerabilities in Initial Access, Execution, and Exfiltration tactics due to insufficient security controls and network segmentation visible in the provided architecture.

Initial Access (TA0001)

Summary: The architecture shows direct internet exposure creating multiple initial access vectors for attackers.

Threat ID	Threat Description	Document Evidence	Example from Documentation	Likelihood	Impact	Risk Score	Recommended Mitigation
T1190	Exploit Public-Facing Application	Doc: samplearchitecture.png, Web tier	Web application directly accessible from internet without visible security controls	5	5	**25-CRITICAL**	Implement WAF, DDoS protection
T1078	Valid Accounts	Doc: samplearchitecture.png, Access paths	No visible authentication/authorization controls in architecture	4	4	**16-HIGH**	Multi-factor authentication, identity management

Execution (TA0002)

Summary: The AI application components appear vulnerable to code execution attacks due to lack of visible isolation controls.

Threat ID	Threat Description	Document Evidence	Example from Documentation	Likelihood	Impact	Risk Score	Recommended Mitigation
T1059	Command and Scripting Interpreter	Doc: samplearchitecture.png, Application layer	AI application likely processes user input without visible sandboxing	4	5	**20-CRITICAL**	Input validation, sandboxing, container security
T1203	Exploitation for Client Execution	Doc: samplearchitecture.png, Web interface	Frontend components accessible without apparent security controls	3	4	**12-HIGH**	Content Security Policy, input sanitization

Persistence (TA0003)

Summary: Database and application tiers lack visible access controls, enabling persistent access establishment.

Threat ID	Threat Description	Document Evidence	Example from Documentation	Likelihood	Impact	Risk Score	Recommended Mitigation
T1505	Server Software Component	Doc: samplearchitecture.png, Backend services	No visible security monitoring of application components	3	4	**12-HIGH**	Application security monitoring, integrity checks

Exfiltration (TA0010)

Summary: Lack of network segmentation and data flow controls create significant exfiltration risks.

Threat ID	Threat Description	Document Evidence	Example from Documentation	Likelihood	Impact	Risk Score	Recommended Mitigation
T1041	Exfiltration Over C2 Channel	Doc: samplearchitecture.png, Network architecture	No visible network monitoring or data loss prevention controls	4	5	**20-CRITICAL**	Network monitoring, DLP, egress filtering

---

SPECIALIZED RISK ASSESSMENTS

Summary: The architecture review reveals significant risks across all specialized areas, with particular concerns around AI model security, data protection, and infrastructure hardening due to the simplified architecture lacking comprehensive security controls.

Agentic AI Risk

Summary: The AI components shown in the architecture lack visible isolation and security controls, creating risks for model manipulation and autonomous system compromise.

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-AGE-001	Doc: samplearchitecture.png, AI components	AI processing components directly connected to web layer	Model poisoning through direct access	4	5	**P0**	Implement model isolation, input validation
T-AGE-002	Doc: samplearchitecture.png, Data flow	No visible model versioning or rollback capability	Compromised model deployment	3	4	**P1**	Model versioning, deployment controls

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-AGE-003	Doc: samplearchitecture.png, Processing layer	AI components lack visible resource constraints	Resource exhaustion attacks	3	3	**P2**	Resource limiting, monitoring

Model Risk

Summary: The architecture shows AI models potentially exposed without proper access controls or monitoring, creating significant model security risks.

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-MOD-001	Doc: samplearchitecture.png, AI layer	AI models appear directly accessible from application layer	Model theft/extraction	4	5	**P0**	Model encryption, access controls
T-MOD-002	Doc: samplearchitecture.png, Input paths	No visible input validation for AI components	Adversarial input attacks	4	4	**P1**	Input sanitization, anomaly detection
T-MOD-003	Doc: samplearchitecture.png, Model components	No visible model performance monitoring	Model drift/degradation	3	3	**P1**	Model monitoring, performance baselines

Data Security Risk

Summary: The architecture lacks visible data encryption, access controls, and segregation between data tiers, creating significant confidentiality and integrity risks.

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-DAT-001	Doc: samplearchitecture.png, Database tier	Database appears directly accessible from application without visible encryption	Data breach through database compromise	5	5	**P0**	Database encryption, access controls
T-DAT-002	Doc: samplearchitecture.png, Data flows	No visible data classification or handling controls	Unauthorized data access	4	4	**P0**	Data classification, access logging
T-DAT-003	Doc: samplearchitecture.png, Storage components	No visible backup or recovery mechanisms	Data loss/corruption	3	4	**P1**	Backup strategy, point-in-time recovery

Infrastructure Risk

Summary: The cloud infrastructure lacks visible security hardening, monitoring, and redundancy controls, creating significant availability and security risks.

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-INF-001	Doc: samplearchitecture.png, Network architecture	Single-tier network design without segmentation	Lateral movement after breach	4	5	**P0**	Network segmentation, micro-segmentation
T-INF-002	Doc: samplearchitecture.png, AWS components	No visible security services (CloudTrail, GuardDuty)	Undetected attacks	4	4	**P1**	AWS security services, SIEM integration
T-INF-003	Doc: samplearchitecture.png, Load balancing	Limited visible redundancy/failover	Service availability attacks	3	3	**P1**	Multi-AZ deployment, auto-scaling

Compliance Risk

Summary: While no specific compliance requirements are stated, the architecture lacks fundamental security controls that would be required for most regulatory frameworks.

Threat ID	Evidence Source (Doc)	Example from Docs	Threat	Likelihood	Impact	Risk Priority	Mitigation Strategy
T-COM-001	Doc: samplearchitecture.png, Overall architecture	No visible audit logging or compliance controls	Audit failures if compliance required	3	3	**P2**	Comprehensive logging, audit trails
T-COM-002	Doc: samplearchitecture.png, Access controls	No visible identity management	Access control violations	3	3	**P2**	Identity and access management

---

COMPONENT-SPECIFIC THREAT ANALYSIS

Summary: Analysis of individual architecture components reveals critical security gaps at each tier, with the web frontend lacking protection, the application layer missing security controls, and the database tier vulnerable to direct access attacks.

Component	Document Evidence	Example from Docs	Critical Threats	Risk Level	Mitigation Approach
Frontend/UI	Doc: samplearchitecture.png, Web interface	Web application directly exposed to internet	XSS, CSRF, DDoS attacks	**CRITICAL**	WAF, CDN, input validation
Backend/App	Doc: samplearchitecture.png, Application servers	Application tier lacks visible security controls	Code injection, authentication bypass	**CRITICAL**	Application security, authentication
Database/Data	Doc: samplearchitecture.png, Data storage	Database appears in same security zone as application	SQL injection, data exfiltration	**CRITICAL**	Network isolation, encryption
AI/ML Models	Doc: samplearchitecture.png, AI components	AI models directly connected without isolation	Model theft, poisoning attacks	**HIGH**	Model security, access controls
Network Layer	Doc: samplearchitecture.png, Network topology	Flat network architecture visible	Lateral movement, network attacks	**HIGH**	Network segmentation, monitoring

---

ATTACK SCENARIOS & KILL CHAINS

Summary: The architecture's security gaps enable multiple high-probability attack scenarios, with the most likely being direct web application compromise leading to full system access due to insufficient network segmentation and access controls.

Scenario 1: Web Application Compromise to Full System Access

Summary: Attackers exploit the directly exposed web application to gain initial access, then leverage the flat network architecture to access AI models and databases without detection.

Kill Chain Phase	Document Evidence	Example from Docs	Description	Detection Window	Mitigation Strategy
Reconnaissance	Doc: samplearchitecture.png, Public exposure	Web application directly accessible from internet	Port scanning, service enumeration	Hours-Days	Network monitoring, threat intelligence
Initial Access	Doc: samplearchitecture.png, Web tier	No visible WAF or input validation	Web application vulnerability exploitation	Minutes-Hours	WAF, input validation, security testing
Lateral Movement	Doc: samplearchitecture.png, Network design	Flat network architecture shown	Direct access to database and AI components	Minutes-Hours	Network segmentation, access controls
Exfiltration	Doc: samplearchitecture.png, Data flows	No visible data monitoring	AI models and data theft	Hours-Days	Data loss prevention, monitoring

---

COMPREHENSIVE RISK MATRIX

Summary: Risk scoring based on likelihood (1-5) and impact (1-5) scales, with the majority of findings scoring in **CRITICAL** and **HIGH** ranges due to the production environment criticality and current security control gaps.

Risk Score Calculation

Likelihood (L)	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Very Likely
5 - Catastrophic	5	10	15	20	**25-CRITICAL**
4 - Major	4	8	12	**16-HIGH**	**20-CRITICAL**
3 - Moderate	3	6	**9-MEDIUM**	**12-HIGH**	**15-HIGH**
2 - Minor	2	4	6	8	10
1 - Insignificant	1	2	3	4	5

All Findings Risk Matrix

Finding ID	Description	Likelihood	Impact	Risk Score	Risk Level	Priority	Owner	Remediation Timeline
F001	Public Internet Exposure	5	5	25	**CRITICAL**	**P0**	Security Team	0-30 days
F002	Insufficient Network Segmentation	5	5	25	**CRITICAL**	**P0**	Infrastructure Team	0-30 days
F003	Missing Security Controls	4	4	16	**HIGH**	**P1**	Security Team	30-90 days
F004	AI Model Protection Gaps	4	4	16	**HIGH**	**P1**	AI/ML Team	30-90 days
F005	Single Points of Failure	3	4	12	**HIGH**	**P1**	Infrastructure Team	30-90 days
F006	Data Encryption Gaps	4	5	20	**CRITICAL**	**P0**	Data Team	0-30 days
F007	Monitoring Deficiencies	3	3	9	**MEDIUM**	**P2**	Security Team	90+ days
F008	Access Control Weaknesses	4	4	16	**HIGH**	**P1**	Identity Team	30-90 days

---

PRIORITIZED RECOMMENDATIONS

Summary: Remediation strategy focuses on immediate critical vulnerabilities affecting system availability and data security, followed by high-priority security enhancements to establish comprehensive protection across all system components.

P0 - CRITICAL (Remediate in 0-30 days)

These findings represent immediate threats requiring urgent action.

Rec ID	Recommendation	Current Risk	Risk Reduction	Implementation Steps	Required Effort	Owner	Target Completion
R001	Implement Web Application Firewall	Critical	80%	1. Deploy AWS WAF, 2. Configure rules, 3. Test and tune	2 weeks	Security Team	Week 2
R002	Establish Network Segmentation	Critical	85%	1. Create VPC subnets, 2. Configure security groups, 3. Implement NACLs	3 weeks	Infrastructure Team	Week 3

Rec ID	Recommendation	Current Risk	Risk Reduction	Implementation Steps	Required Effort	Owner	Target Completion
R003	Encrypt Data at Rest and in Transit	Critical	75%	1. Enable database encryption, 2. Configure TLS, 3. Key management	2 weeks	Data Team	Week 2

P1 - HIGH (Remediate in 30-90 days)

High-priority improvements that significantly reduce risk exposure.

Rec ID	Recommendation	Current Risk	Risk Reduction	Implementation Steps	Required Effort	Owner	Target Completion
R010	Deploy Security Monitoring	High	70%	1. Enable CloudTrail, 2. Configure GuardDuty, 3. Set up alerting	4 weeks	Security Team	Week 6
R011	Implement AI Model Security	High	65%	1. Model encryption, 2. Access controls, 3. Versioning	6 weeks	AI/ML Team	Week 8
R012	Multi-Factor Authentication	High	60%	1. Deploy identity provider, 2. Configure MFA, 3. User training	4 weeks	Identity Team	Week 6
R013	Backup and Recovery	High	50%	1. Automated backups, 2. Recovery procedures, 3. Testing	4 weeks	Infrastructure Team	Week 6
R014	Input Validation and Sanitization	High	65%	1. Code review, 2. Validation libraries, 3. Testing	6 weeks	Development Team	Week 8

P2 - MEDIUM (Remediate in 90+ days)

Medium-term strengthening measures for comprehensive security.

Rec ID	Recommendation	Current Risk	Risk Reduction	Implementation Steps	Required Effort	Owner	Target Completion
R020	Enhanced Logging and SIEM	Medium	40%	1. Centralized logging, 2. SIEM deployment, 3. Correlation rules	8 weeks	Security Team	Week 12
R021	Penetration Testing	Medium	30%	1. Vendor selection, 2. Testing execution, 3. Remediation	6 weeks	Security Team	Week 10
R022	Disaster Recovery Plan	Medium	35%	1. DR procedures, 2. Site setup, 3. Testing	8 weeks	Infrastructure Team	Week 12

Rec ID	Recommendation	Current Risk	Risk Reduction	Implementation Steps	Required Effort	Owner	Target Completion
R023	Security Training Program	Medium	25%	1. Training development, 2. Delivery, 3. Assessment	10 weeks	HR/Security	Week 14

SECURITY CONTROLS MAPPING

Summary: Security controls mapped to NIST SP 800-53 framework to address identified findings, with current implementation gaps requiring immediate attention across access control, system integrity, and incident response categories.

Control Category	Control Name	Implementation Status	Addresses Finding	Compliance Requirement	Timeline
Preventive	Access Control (AC-3)	Not Started	F001, F008	NIST SP 800-53	30 days
Preventive	System and Communications Protection (SC-7)	Not Started	F002	NIST SP 800-53	30 days
Preventive	Identification and Authentication (IA-2)	Not Started	F008	NIST SP 800-53	60 days
Detective	Audit and Accountability (AU-2)	Not Started	F003, F007	NIST SP 800-53	90 days
Detective	System and Information Integrity (SI-4)	Not Started	F003, F004	NIST SP 800-53	60 days
Responsive	Incident Response (IR-4)	Not Started	All Findings	NIST SP 800-53	90 days
Preventive	System and Services Acquisition (SA-8)	Not Started	F004	NIST SP 800-53	90 days
Preventive	System and Communications Protection (SC-8)	Not Started	F006	NIST SP 800-53	30 days

---

COMPLIANCE CONSIDERATIONS

Summary: While no specific compliance requirements are mandated, the current architecture would fail most regulatory frameworks due to insufficient security controls, requiring comprehensive remediation for future compliance readiness.

Finding ID	Finding	Compliance Requirement	Compliance Gap	Required Evidence	Remediation Timeline
F001	Public Internet Exposure	None	Would violate PCI DSS if handling payment data	Network segmentation documentation	30 days
F002	Network Segmentation	None	HIPAA violation if handling health data	Network architecture diagrams	30 days

Finding ID	Finding	Compliance Requirement	Compliance Gap	Required Evidence	Remediation Timeline
F003	Missing Security Controls	None	SOX compliance issues if financial data	Security control documentation	90 days
F006	Data Encryption	None	GDPR violations if EU personal data	Encryption implementation records	30 days
F007	Monitoring Deficiencies	None	SOC 2 Type II failures	Audit logs and monitoring evidence	90 days
F008	Access Control	None	Most frameworks require access controls	Identity and access management records	60 days

---

REFERENCES

Threat Modeling Frameworks:

- **MITRE ATT&CK** - Comprehensive framework for understanding cyber adversary behavior

- Focus: Tactics, Techniques, and Procedures (TTPs)

- Coverage: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Impact

Security Standards & Guidelines:

- [NIST SP 800-53 Rev 5](https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) - Security and Privacy Controls for Information Systems and Organizations

- [OWASP Top 10 2021](https://owasp.org/www-project-top-ten/) - Top 10 Web Application Security Risks

- [MITRE ATT&CK Framework](https://attack.mitre.org/) - Adversary Tactics, Techniques, and Common Knowledge

- [CIS Critical Security Controls v8](https://www.cisecurity.org/controls/v8) - Critical Security Controls for Effective Cyber Defense

- [ISO/IEC 27001:2013](https://www.iso.org/standard/54534.html) - Information Security Management Systems Requirements

Compliance Frameworks:

- **None** - No specific regulatory compliance framework required

Risk Assessment Methodologies:

- [CVSS v3.1](https://www.first.org/cvss/v3.1/specification-document) - Common Vulnerability Scoring System

- [FAIR](https://www.fairinstitute.org/) - Factor Analysis of Information Risk

- [NIST Risk Management Framework (RMF)](https://csrc.nist.gov/projects/risk-management/about-rmf) - NIST Risk Management Framework

Additional Resources:

- [CERT Secure Coding Standards](https://wiki.sei.cmu.edu/confluence/display/seccode) - Carnegie Mellon SEI Secure Coding

- [SANS Top 25 Most Dangerous Software Errors](https://www.sans.org/top25-software-errors/) - SANS CWE Top 25

- [Cloud Security Alliance (CSA) Cloud Controls Matrix](https://cloudsecurityalliance.org/research/cloud-controls-matrix/) - CSA CCM

- [ENISA Threat Landscape Reports](https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends) - European Union Agency for Cybersecurity

---

DISCLAIMER

AI-Generated Report Notice:

This threat assessment report was generated using artificial intelligence (AI) technology powered by SecureAI. While the analysis incorporates industry-standard frameworks, best practices, and uploaded documentation, it should be considered as a preliminary assessment tool.

Important Considerations:

- This report is AI-generated and may contain inaccuracies, omissions, or misinterpretations
- All findings, risk ratings, and recommendations must be validated by qualified security professionals
- The assessment should be reviewed and supplemented with manual security analysis
- Implementation of any recommendations should be evaluated in the context of your specific environment
- This report does not replace professional security audits, penetration testing, or compliance assessments

Recommended Next Steps:

1. Review this report with your security team and subject matter experts
2. Validate findings against your actual system architecture and controls
3. Conduct additional manual threat modeling sessions
4. Perform security testing to confirm identified vulnerabilities
5. Engage certified security professionals for critical systems

By using this AI-generated report, you acknowledge that it serves as a starting point for threat modeling activities and requires human expertise for validation and implementation.